NATO Communications and Information Agency

Costed Customer Services Catalogue

V3.4

NATO OTAN

This page is left blank intentionally

Table of Contents

Introduction to the NCI Agency Costed Customer Services Catalogue

The NCI Agency Costed Customer Services Catalogue provides a unique, exhaustive and standardised list of Services which are offered to the customer in support of their achievement of specific business outcomes and objectives. The NATO enterprise is complex and extensive; comprised of many different geographically dispersed customers and entities, spanning a wide spectrum of requirements and needs. The NCI-Agency Costed Customer Services Catalogue reflects this complexity by providing a wide range and variety of services, service variations (flavours), value added services, and products. As such, the Costed Customer Services Catalogue forms a true representation of the diverse needs of customers.

The Catalogue constitutes a living document which adapts and matures as customer requirements evolve and change over time. Maintaining a proper alignment between both services and customer requirements is a key principle which enables the NCI Agency to support and add value to customer business. This catalogue has been build and structured on the basis of a customer-centric approach and in accordance with standards and definitions in industry best practise.

The NCI Agency Costed Customer Services Catalogue constitutes primarily a list of Services. However, many of the services in the catalogue can also be offered in the form of a product. To this end, the Agency enclosed a supplemental product catalogue which complements the service catalogue. The product catalogue allows the NCI Agency to remain flexible towards the needs and objectives of customers. Moreover, it provides the means to cater to a larger and more distinct group of customers who, either for technical reasons or business motives, are not able to consume services. The NCI Agency Costed Customer Services Catalogue is therefore comprised of two distinct but paired catalogues, i.e. the Services Catalogue and the Products Catalogue. This introductory note explains the concepts of “services”, “products” and “value added services” for the convenience and understanding of the customer in the use of this Catalogue.

Service

ITIL defines a service as a set of related functions provided by IT systems in support of one or more business areas, which in turn may be made up of software, hardware and communications facilities, perceived by the customer as a coherent and self-contained entity. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. Additionally, ITIL specifies that an IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement[1]. In essence, a service delivers an intangible benefit[2], either in its own right or as a significant element of a tangible product. For example, the provisioning of the NCOP functional application service provides customers with an increased situational awareness on the battlespace, increased collaboration and ultimately improved military operations. As opposed to products, the concept of providing a service is not limited to the delivery a specific tangible or intangible system, but rather the provisioning of a whole set of logically related processes, activities, infrastructure, technologies, which in combination with specific skills and knowledge, is able to add value by facilitating customer’s business outcomes and goals. Therefore, when we refer to services, we do not just include the provisioning of a specific solution or product, but in addition, include all activities related to the deployment, configuration, management, maintenance and operation.

[1] ITIL V3 definition of a Service.

[2] These benefits (outcomes) are generally difficult to measure and quantify and as such are mostly referred to as “intangible”.

Together, as a packaged whole, they denominate and qualify the concept of a Service. Ultimately, a service provides a level of abstraction, which allows the customer to focus on outputs and outcomes without incurring any intrinsic risks related to the operation and maintenance of the service. When services are priced[1] they incorporate all cost elements which are related to the provisioning of a service (operation and maintenance), both in terms of manpower and external CIS costs.

Services within the NCI Agency Costed Customer Services Catalogue are categorised into 9 different groups, commonly referred to as "Service Portfolio Groupings", these are:

- Workplace Services
- Infrastructure Services
- Platform Services
- Subject Matter Expertise Services
- Application Services
- Logistic Support Services
- Security Services
- Training Services
- Other Services

Product

As opposed to services, Products are tangible and discernible items, which are delivered as physical assets or intangible assets. While a product is something that can be quantified, a service is less concrete and is the result of the application of skills and expertise towards an identified and specific objective. Most commonly products are delivered in the form of an unmanaged device (e.g. Laptops, desk computers, phones, smartphones, etc.) or software application (e.g. functional applications and specialist applications). Contrary to services, these products will be delivered in a standalone state, without any support in terms of installation, configuration, maintenance and operation. Moreover, especially for functional applications, where the underlying infrastructure is not owned or operated by NCI-Agency. The price for a product therefore equates to its base cost of acquisition. In some instances where standardisation is of no or little importance, i.e. COTS Software, customers are free to purchase the product via their own channels.

Value Added Service

By themselves, products do not satisfy any specific and immediate business need or objective. Only when deployed, configured, maintained and operated they can be used in support of certain business activities. In order to cater for the eventuality where such additional activities are required, NCI-Agency has created the concept of Value Added Services. As the name suggest, value added services enhance and complement specific products, and in some instances services[4]. The product in combination with all or some of its value added services therefore equates to its service counterpart[2]. From a pricing perspective, value added services are mostly, if not exclusively, comprised of costs, which are related to human resources. The cost of a value added service is therefore dependant on the number of manpower units (FTE) that are needed to execute and deliver specific activities. Value

[1] NCI Agency is costing or pricing the Services in accordance with the Customer Funding Regulatory Framework.

[2] It should be noted that in some instances, as for example with mentoring and training which qualify as "value added service", customers who have opted for the service are still eligible to purchase these value added services.

added services are referred to as services because they exclusively consist of the delivery of specific NCI-Agency expert skills and knowledge. They are however quite distinct from the services which were defined earlier. Therefore, the NCI-Agency Customer Service Catalogue will group all of the value added services in a separate list in the future.

Value added services can be provided for a number of areas or activities:

- Installation & Configuration
- Release Management (Patch and version releases)
- In-Service-Support (Level 1,2 and 3)
- Mentoring
- Training
- Project Support
- Auditing

Service & Product Attributes

The NCI Agency Costed Customer Services Catalogue adopted a standardised template for describing services and products. A description comprises a specific set of attributes, which define and qualify the service or product. The description templates have been designed from a business and customer centric point of view. Following table lists and defines all attributes, which are valid for Product and/or Service.

#	Attribute name	Attribute Description	Applicable to:	
			Product	Service
1	Service/Product ID code	6 character code, which uniquely identifies a service or product. Customers can use this code to refer to specific service or product.	X	X
2	Service/Product Name	Short name designating the service or product.	X	X
3	Portfolio Group	Indicates the Service Portfolio Group to which the service in question belongs.	X	X
4	Service/Product Status	Indicates the Portfolio status of the Service or product, i.e. “Pipeline”, “Available” or “Retired”.	X	X
5	Service/Product description	Describes the service or product from a non-technical perspective.	X	X
6	Value Proposition	Explains in business terms how a service or product supports specific business processes and as such facilitates specific business outcomes and objectives.	X	X
7	Service/Product Features	Lists and describes the features of the service or products. Complements the service description.	X	X
8	Service/Product Request	Describes the procedure, which is required for customers to request the service or product.	X	X

		Describes the means by which customers can report incidents and problems related to the use of the service or product.		
9	Service/Product Flavours	Describes the different variations in which a service or product can be offered.	X	X
10	Available Networks	Lists the security environments in which the service or product is available, i.e. NU – NU – NS – MS, on which the service can be delivered.	X	X
11	Service/Product Prerequisites	Lists the services, which are required beforehand in order to consume the service in question. The Customer needs to ensure that the prerequisite service are in place. For products, this section will be dedicated to system prerequisites.		X
12	Standard Service Support levels	Details the availability target for the service, i.e. the time the service is available to the customer considering the potential downtime of a service. This figure does not include any maintenance activities. Details the restoration time for a service, i.e. the maximum time which is needed to restore the service in the eventuality of a major or critical incident.	X	X
13	Support Hours	Details the times during which helpdesk support (including level 2 and 3 support) is available for the customer.		X
14	Service/Product Cost	Describes the unit of measure, which is used in the calculation of the service price. Describes the Service price and the constituent cost elements, which make up the price. This attribute will only detail the base acquisition price for products.	X	X

Unless otherwise specified in a specific service definition sheet, the following attributes are equally valid for all services in the Catalogue:

Service Status: Available

Support Hours:

- Centralized Service Desk specialist agents are available Mon-Thurs 06.00-22.00 CET, Fri 06.00-20.00 CET. Outside of these hours, calls to the CSD will be answered by 24/7 duty Ops Centre personnel who will record the Incident/Service Request and take escalation action if necessary.
- Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Requests

- **Incident/problem reporting:**
  Contact Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177, Netherlands +31 70 374 3177, Italy +39 081 721 3177 or Germany +49 282 4978 3177
For NATO HQ +32 02 707 5858

- **New Service Request:**
  Please complete Customer Request Form and contact NCI Agency Demand Management.

NCI Agency Education and Training

NCI Agency provides a comprehensive set of C4ISR and Cyber education and training courses. These are provided either at the NATO CIS School (NCISS) or at other Agency's locations, or delivered by a mobile training team at the site of the customer. An overall overview of available C4ISR and Cyber courses may be accessed at https://www.ncia.nato.int/Our-Work/Pages/Education-and-Training.aspx.

The NCI Agency education and training courses are not an element of this Catalogue, except for the information on the total cost of NCISS services available to NATO Command Structure, which is an element of the Service Rates document.

This page is left blank intentionally

COSTED CUSTOMER SERVICES CATALOGUE – SERVICE DEFINITION SHEETS

V3.4

This page is left blank intentionally

.

WORKPLACE SERVICES

V3.4

This page is left blank intentionally

WPS001 - Managed Device Service

Service ID: WPS001

Service Name: Managed Device Service

Portfolio Group: Workplace Services

Service Description: The Managed Device Service provides the user with a client device (various form factors) that allows them to connect to the NATO network (on the specific security domain). The Service includes full office automation software (MS Office Professional Suite), Windows operating system and NATO recommended security tools.

Value Proposition: The Managed Device Service offers the user a fully managed device for office automation, browsing and application access. This allows users to connect, interact and collaborate with other users and supports business activity including the production of documentation and presentations, etc. This aids operational efficiency, effectiveness and supports all business processes throughout the enterprise.

Service Features: The Managed Device Service includes a fully managed hardware device (Desktop, Thin Client, Laptop, Tablet or smart phone), MS Operating system, Office automation software (MS Office Professional suite), Web Browser, NATO recommended security tools and PDF Reader software. The managed devices also provides controlled peripheral access (e.g. USB storage devices). Headsets and USB cameras are optionally available in addition to the standard service offering.

Service Flavours:

Static (Thick or Thin) Desktop device – This service flavour provides the user with a desktop device that needs to be connected to a wired network. The desktop device features a TFT display (min 19") connected and keyboard and mouse. There is an option for an additional LCD Monitor and KVM. Exceptionally, a thick client can be provided as a standalone device.

Common use thin client device – This service flavour is only applicable for the New NATO HQ and provides a device for common use (e.g. public areas, conference rooms etc.).

Portable (Laptop/Tablet Device) - This service flavour provides the user with a Laptop device that needs to be connected to either a wired or wireless network directly or through remote access. The laptop comes with a power supply, a carrying case and an external mouse. This service flavour is intended for users that require mobility (remote access) in combination with desktop-like user experience.

There is an option for a Static work position which consists of a docking station, LCD Monitor, Keyboard and mouse.

NAC Tablet devices[1]: This service flavour provides tablets configured and maintained specifically for NAC meetings. The tablet includes a Wi-Fi dongle which allows connection to the NAC secured Wi-Fi network (local network via secured Wi-Fi specifically for NAC meetings).

Mobile (Smart Phone Device) - This service flavour provides the user with a smartphone device that needs to be connected to a wireless network directly or through remote access. This service flavour is intended for users that require mobility (remote access). The voice subscription is not part of the service flavour, it should be obtained separately.

[1] Please note that, while the "NAC Tablet" service includes level 1 - 2 - 3 support and maintenance, Level 1 support is partially shared between NCIA – CSU Brussels and NATO IS staff.

Available on:

Static (Thick or Thin) Desktop device:
NATO Secret
NATO Restricted
NATO Unclassified
Mission Secret
NATO Partner network (For NNHQ)
Standalone (Not connected to NATO network)
Portable (Laptop/Tablet Device):
NATO Secret
NATO Restricted
NATO Unclassified
NATO Partner network (For NNHQ)
NAC Tablet devices[1]:
NAC Network
Mobile (Smart Phone Device):
NATO Restricted
NATO Unclassified

Service Prerequisites:

INF001 - LAN Service
WPS002 - User Access Service
WPS003 - Enterprise User License Service

Standard Service Support Levels:

Service Availability[2] Target: 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is Per Device.

[1] Please note that, while the "NAC Tablet" service includes level 1 - 2 - 3 support and maintenance, Level 1 support is partially shared between NCIA – CSU Brussels and NATO IS staff.
[2] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS002 - User Access Service

Service ID: WPS002

Service Name: User Access Service

Portfolio Group: Workplace Services

Service Description: The User Access Service provides users with an identity (e.g. username and password) to access the enterprise network on the various NATO Domains. Additionally, the service includes the provisioning of personal storage space (minimum 20 GB on default) for storing user profile files, personal information and documents. Additional physical components, i.e. tokens, smart cards containing the required authentication certificates are available, in order to logon to the applicable network and access necessary resources.

Value Proposition: The User Access Service allows the users to securely access different NATO networks, and it enables the NCI Agency to control access to accounts, usernames and passwords using all other services, as well as to track and control usage of services ensuring only authorized users are accessing relevant services. Furthermore, it enables enhanced security, prevention of oversubscription to services, and control of licensing.

Service Features: The User Access Service is available for all relevant services requiring authentication. Access is usually provided by creation of a username and password, with an authentication token available as stronger authentication option. Additionally, User Access Service provides the remote-access authentication (mobility) of Managed Devices (Portable devices and Mobile Phones).

Service Flavours: The service is available in a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability
Service Restoration: Where the service deems unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is Per Account. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS003 - Enterprise User License Service

Service ID: WPS003

Service Name: Enterprise User License Service

Portfolio Group: Workplace Services

Service Description: The Enterprise User License service provides a Microsoft Enterprise License based on NATO User Profile which comes in two pre-packaged profiles (NATO light and NATO Standard) of which both contain the same licensing components and the same functionality to the user, however with different number of qualified devices that the licenses are allowed to run on.

Value Proposition: This service allows users to access via multiple devices (desktop, laptop, thin clients…), on multiple networks (business, operational, missions & exercises), and also to leverage the mobile devices that are increasingly typifying our environment (phones, tablets, iOS, Android). This user approach achieves both of the aims of reduced cost, and simplified licensing and management.

Service Features: The key licensing components cover the core business needs of the users for Windows Office and server access across the NATO Enterprise. The licensing components included are:

- Windows: Windows Software Assurance per user provides access to Windows Enterprise for install or VDI across devices
- MS Office: On-premise version of MS Office Professional Plus Suite across Windows devices
- Enterprise Client Access: enterprise client access licenses to access the server functionality in Windows, Exchange, SharePoint per user across devices
- SQL Client Access: Client access to SQL Server per user across devices
- Skype for Business Plus Client Access: Client access to enterprise-grade instant messaging and phone features in Skype for Business per user.

Service Flavours: The Enterprise User License Service is available in the following flavours:

- **User-based License:**
  NATO Light Profile authorizes use of the licensed Products on **up to 2 (two)** Qualified Devices[1] whereas at least one of those Qualified Devices is connected to the internet.
  NATO Standard Profile authorizes use of the licensed Products on **up to 5 (five)** Qualified Devices.
- **Subscription-based Device License**[2] is applicable where the subscription to licenses is based on devices instead on users.

Available on:

NATO Unclassified

[1] "Qualified device" is any personal desktop computer, portable computer, workstation, or similar device (excl. Smartphones) used by or for the benefit of any Affiliate included in its Enterprise and that meets the minimum requirements for running any of the Enterprise Products.

[2] Subscription-based device license is not a perpetual license and hence ceases to exist once the annual cost ceases to be paid. Therefore, a subscription-based license cannot be transferred back and be used for national purposes afterwards.

NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is Per User or Per Device, depending on the flavour. Price details available in the Service Rates Document.

WPS004 - E-mail Service

Service ID: WPS004

Service Name: E-mail Service

Portfolio Group: Workplace Services

Service Description: The e-mail Service provides the user with access to the NATO e-mail system, including the provision of one or more mailboxes, on the relevant domain, allowing the user to send and receive e-mail messages and attachments.

Value Proposition: The e-mail Service allows users to send and receive e-mails on the relevant domain. This significantly reduces time and cost of communication, supporting all business process across the enterprise.

Service Features: Standard MS Exchange Mailbox. This mailbox is accessible through a thick mail client (outlook) or through the web-based client. Mailboxes are available to support individuals or groups; e.g. personal mailbox, functional mailbox or group mailbox.

Service Flavours: The service is available as a single flavour. The standard mailbox size is 10GB.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service Prerequisites:

WPS001 - Managed Device Service (or qualified connected device)
WPS002 – User Access Services
WPS003 - Enterprise User License Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is Per Mailbox. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS005 - Instant Messaging Collaboration Service

Service ID: WPS005

Service Name: Instant Messaging (IM) Services

Portfolio Group: Workplace Services

Service Description: IM Services allow a user to collaborate with other users, using instant text messages. The IM Service also informs other users about the presence of the user. Multiple users can be invited into chat rooms to discuss relevant topics.

Value Proposition: IM Services reduce the time taken and cost of communicating with other users. The Service supports collaborative working and facilitates discussion between multiple parties without the requirement of being collocated.

Service Features: IM Service provides a soft client on a user's device, allowing them to check the availability of other users and to send instant text messages. The IM client supports 1-2-1 chats, group conversations and desktop sharing. The service is based on Skype for Business.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret
NATO Restricted
NATO Unclassified
Mission Secret (only in Exercise environment)
NATO Partner network (For NNHQ)

Service Prerequisites:

WPS001 – Managed Device Service (or qualified connected device)
WPS002 – User Access Services
WPS003 – Enterprise User License Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Cost / Price: The unit of measure for the service is Per Account. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS006 - REACH Mobile Workplace Service

Service ID: WPS006

Service Name: REACH Mobile Workplace Service

Portfolio Group: Workplace Services

Service Description: The REACH Mobile workplace Service provides the user with a NATO client device (Laptop/Tablet/Smartphone) that allows them to connect to the NATO RESTRICTED network. Additionally The Service includes:

- A User Account, Password and PKI token to access the NR.AIS Network (WPS002)
- A mailbox on the Restricted network (WPS004),
- An IM Collaboration Account (WPS005),

The Laptop Client device is loaded with the office automation software (MS Office Professional Suite), Windows operating system, VPN client software and security and management tools. The Smartphone Client device is loaded with IM collaboration software, and E-mail client, a web browser, VPN client software and security and management tools.

Value Proposition: The REACH Mobile workplace service is a bundle of 4 services (Managed Device Service, User Access Service, E-mail Service, IM collaboration Service) offered as a single service package for the NATO Restricted Network.

Service Features: Same as the 4 individual services comprised in this service offer. There is an additional option for a Static work position which consists of a docking station, dual LCD Monitor, VTC camera, Keyboard and mouse. (This option is only applicable for the Portable Client Device service flavour).

Service Flavours:

Portable Client Device (Laptop) - This service flavour provides the user with a Laptop device that needs to be connected to either a wired or wireless network. The laptop comes with a power supply, a carrying case, a headset and an external mouse.

Optional Static Work position – this option is only applicable for a portable client device service flavour; it provides the user with a docking station for the portable device, dual LCD monitor, a VTC camera, keyboard and mouse.

Mobile Client Device (Smartphone) This service flavour provides the user with an Apple iPhone device. This device can connect to both cellular and WiFi networks. The cellular subscription (Voice and Data) is not included in the standard service offer and needs to be added on top.

Available on:

NATO RESTRICTED

Service Prerequisites:

WPS003 - Enterprise User License Service

Standard Service Support Levels:

Service Availability[1] **Target :** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Cost / Price: The unit of measure for the Service is Per Device. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS007 - Print/ Scan/ Copy Service

Service ID: WPS007

Service Name: Print/ Scan/ Copy Service

Portfolio Group: Workplace Services

Service Description: Print, scan and copy services enable user to create hardcopies of digital content or digitize hardcopies. Under this service, NCI Agency will provide either NATO owned or outsourced (leased) devices. These devices will be deployed in the user environment and allow users to print/scan or copy from any device. Some networks support badge controlled pull printing.

Value Proposition: The Print/ Scan/ Copy Service supports all business Process across the enterprise. It allows production of documentation and sending it to individuals and organizations who do not have access to the relevant security domain (including the production of multiple copies for meetings etc.). It also allows hard copy documentation (possibly externally produced) to be electronically stored and transmitted on the relevant domain.

Service Features: Different form factors are available. Multi-Functional Printing (MFP) devices which scan/print/copy, individual printers or scanners and plotters are available on all NATO security domains.

Service Flavours:

Large MFP (Printer/ Scanner/Copier) Badge controlled – This device is intended for departmental or large workgroup environments (up to 10k prints per month), it supports up to A3 printing and scanning in colour and B/W. This device prints up to 30 pages per minute in B/W and 30 pages per minute in Colour.

Printer - This device is suitable for office or small workgroup environments (up to 5k prints per month), it supports up to A4 printing in colour and B/W. This device prints up to 20 pages per minute in B/W and 20 pages per minute in Colour.

Customer Owned Printers: Please note that this option is for customers, who have non-NCI Agency owned printers (MFPs, Standalone or Network connected printers), and who would like NCI Agency services only for the installation support of their printers. In this case, service costs for Customer Owned Printers are limited to an initiation fee, which is needed to install the printer. The NCI Agency responsibility for these printers stops after the installation. Customers shall note that the NCI Agency cannot be held accountable for any hardware failure. Any support in terms of maintenance is therefore the responsibility of the customer, including printer consumables and spare-parts.

Scanner - This device is suitable for office or small workgroup environments. It supports up to A4 scanning in colour and B/W

Large Format printer (Plotter) - This device is suitable for specialised graphics printing, it supports up to A0 printing in colour and B/W.

Available on

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

NATO Partner Network (for NNHQ)

Service Prerequisites:

WPS001 - Managed Device Service (or qualified connected device)
For Scanning – WPS004 – E-mail Service

Standard Service Support Levels:

Service Availability[1] **Target :** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS008 - Operations Centre Service

Service ID: WPS008

Service Name: Operations Centre Service

Portfolio Group: Workplace Services

Service Description: The Operations Centre Service is comprised of 2 service functions: 1) Centralised Service Desk (CSD), 2) Network Monitoring and Control Services. Centralised Service Desk (CSD) acts as a single point of contact for authorised users of all Networks, CIS Services and Applications provided by the Agency. The CSD will log, categorize and resolve/escalate and manage all incidents from authorised users. The CSD function is a sub-service of other services the NCI-Agency provides. The CSD comprises sub-elements in the primary and Alternate Operations Centre locations that together form the CSD but the sub-elements can provide the service independently if required. The Network Monitoring and Control Services are provided by the Network Control Centre as an Operations Centre Entity. The NCC is responsible for providing monitoring of all Networks provided by the Agency to Customers for their users. The NCC utilizes event and incident management across the corporate networks and services. NCC provides end-to-end visibility across all networks and services, including Cyber Security services under arrangements with the CS and NS&II SLs. The NCC is a virtual entity with 2 locations Mons and Brunssum, the service can be provided independently if required but the Brunssum site would need reinforcements after 24 hours.

Value Proposition: The Centralized Service Desk will be available as sub-service for all locations via one single telephone extension for any applicable service. Since the CSD will be responsible for all Services and Networks there will be efficiencies in terms of overall costs and Incident/Request resolution times. The full range of the Agency's support capabilities will be available via a single point of contact. The Network Monitoring & Control Services provide centralised event and incident management on any Network NCI Agency provides on a 24/7 basis including at least 1st level support. Through correct event management, incident management is more efficient, reducing services mean time to restore (MTTR).

Service Features: CSD agent will use ITSM ticketing system to log, categorize and escalate to the next support unit all incidents related to CIS services provided by the NCIA. When possible, CSD agent will troubleshoot and solve level 1 issues. The NCC provides visibility of the status of the corporate networks. The NCC utilises DIS provided tools to event manage across the corporate networks to the LANs of the NATO command structure command locations, NATO Force Structure element locations, Operational and Deployed commands.

Service Flavours:

NS / NU: The Service cost is included in the WPS001 Managed Device Service, with NM&C element included.

NR / REACH: The Service cost is included in the WPS006 Reach Mobile Workplace Service, with NM&C element included.

Outside of NATO Enterprise Network: Fixed price for the Service for all networks, level 1 support not included.

Available on: Operations Centre is available for the following Networks:

NATO Unclassified

NATO Restricted
NATO Secret

Minerva and Mission networks currently have their own local Service Desk that will survive as long as the special Network domain exist and/or the CSD can provide the same level of service.

Service Prerequisites:

None

Standard Service Support Levels: The Operations Centre is available 24/7. For The CSD component, following KPIs apply:

Available hours	First Call Resolution[1] Target	Target Time to Pick Up
24/7	75 %	5 minutes

Service Cost / Price: The unit of measure for the Service is Per Workstation. Price details available in the Service Rates Document.

WPS009 - Voice Collaboration Service

Service ID: WPS009

Service Name: Voice Collaboration Service

Portfolio Group: Workplace Services

Service Description: The voice collaboration service provides user with the ability to collaborate and communicate through audio.

Value Proposition: Voice collaboration Services allow easy communication between more than one parties, from any location. This dramatically increases flexibility and saves cost as no travel is required (especially when using conferencing facilities).

Service Features: Different Form Factors (Telephone, IP phone, mobile phones), conferencing, hunt groups, voice mail, phone billing service, call intercept and call forwarding are provided on the available NATO security domains.

Service Flavours: Available flavours are the following:

Desk phone (Static): This provides the users with a static desk phone and a number assigned. The difference between regular phone or VoIP phone depends on the local site infrastructure. The voice subscription is not part of the service, it should be obtained separately.

Mobile phone: This service flavour provides users with a mobile phone device using regular carrier providers as well as Satellite providers to make voice calls. The voice subscription is not part of the service flavour, it should be obtained separately. The voice subscription is not part of the service, it should be obtained separately. The voice subscription is not part of the service, it should be obtained separately.

(This service flavour does not include mobile phones with the data plan subscription. Should a mobile phone include both voice and data plan, it is to be requested through the Managed Device service (WPS001) Smart Phone flavour.)

Soft phone: This service flavour provides users, via the provisioning of a soft client, the ability to place voice calls using managed devices.

Available on:

Desk phone (Static): NATO Unclassified and NATO Secret

Mobile phone: NATO Unclassified

Soft phone: NATO Unclassified and NATO Restricted

Service Prerequisites:

For IP Phone – INF001 - LAN Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5%

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device. Price details available in the Service Rates Document.

WPS010 - Video (VTC) Collaboration Service

Service ID: WPS010

Service Name: Video (VTC) Collaboration Service

Portfolio Group: Workplace Services

Service Description: The Video (VTC) collaboration service provides users the ability to collaborate and communicate through video and audio. It allows users from different geographical location to have face-to-face like collaboration as well as it supports multi-user, multi-location collaboration.

Value Proposition: The Service allows individuals and groups to interact easily, which enables a more flexible and efficient exercise of the Command and Control with significant savings in travel time and cost.

Service Features: The Service features include scheduling, VIP monitoring, conferencing, recording, playback and streaming, and connectivity of third parties.

Service Flavours:

VTC Soft Client: provides users with an application (Polycom RealPresence Desktop) installed on the managed/qualified device. The flavour requires a camera and a microphone (in-built or as addition).

Dedicated Terminal: provides users with a dedicated VTC terminal (Polycom) connected to the network, which can be either:

- Desktop VTC Terminal; or
- Huddle/small room based system.

Conference room VTC: integrates with Conference room setups that become VTC enabled – it's provided with a camera and microphone and can be integrated with Conference room projection and presentation devices. The flavour has a range of room systems depending on their size, number supported participants, and the need for mobility, as follows:

- Roll About VTC system:
  - Single Domain;
  - Dual Domain;
- 15-man room VTC system (dual domain system);
- 25-man room VTC system (dual domain system);
- 50-man room VTC system (dual domain system);
- 175-man room VTC system (dual domain system).

Immersive Telepresence Meeting Room VTC: This service flavour uses enhanced **c**onference room technologies and provides the illusion of an in person meeting through the use of multiple screens in an `across the table` setup. Available only as single domain system.

VTC B2B (Business to Business): provides a possibility to communicate through audio and video between NATO users and external VTC networks such as Nations, Missions, Deployed CIS, NGO's and GO's.

Available on:

NATO Unclassified (including public access)
NATO Restricted

NATO Secret
NATO Partner Network (For NNHQ)

Service Prerequisites:

WPS001 - Managed Device Service (or qualified connected device) for VTC Soft Client Flavour

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Client Device. For price information per flavour, see the Service Rates document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

WPS011 - IP Television (IPTV) Service

Service ID: WPS011

Service Name: IP Television (IPTV)

Portfolio Group: Workplace Services

Service Description: IP Television provides the user with commercial cable television service as well as NATO specific channels. This service provides numerous channels, primarily focused on news and informational events, and offered in a variety of languages used in NATO.

Value Proposition: The IP Television Service offers the user an ability to leverage a fully managed and operated contractor service inside the New NATO Headquarters. This allows the user to keep up to date with news events. In addition to commercial news, the user can also view NATO channels which provide NATO news as well as can provide streamed videos of HQ briefings. This aids operational efficiency and effectiveness and supports situational awareness throughout the headquarters.

Service Features: The IP Television Service includes a fully managed and operated commercial capability augmented with NATO information. IP Television can be a full service providing the television, trolley and channels or as small as offering the channels and a connection SetTopBox (STB).

Business users can access three of the main news channels on their NATO managed mobile device.

Nations and staff can request additional channels that offer specific programming or national specific content. These channels can be ordered separately and the price is based on the requested licensing.

Service Flavours:

IP Television – This service supports the office environment. The 55" television is mounted on a trolley and connected to the floor box plug in a specific office or meeting room

Available on:

Public network

Soft client – This service flavour allows the users to access the IPTV channels from their devices, provided through the managed device services.

Available on:

NATO Restricted

NATO Unclassified

Service Prerequisites:

WPS001 – Managed Device Service (for Soft client Service flavour)

Standard Service Support Levels:

Service Availability[1] **Target:** 99%

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device. Price details available in the Service Rates Document.

#	Channel Name	#	Channel Name
1	La Une	23	CNBC-E
2	La deux	24	Sky news
3	La trois	25	Channel 5
4	France24	26	ITV 1
5	TV5Monde	27	ITV 2
6	BBC World	28	ITV 4
7	MTV	29	BBC News
8	CNN	30	ITV 3
9	Euronews	31	RTP-International
10	Nederland 1	32	RAI News24
11	Nederland 2	33	TVR International
12	Nederland 3	34	ARD
13	BBC1	35	TV-8
14	BBC2	36	ATV
15	National Geographic Channel HD	37	TRT 1
16	RAI 1	38	TRT 2 (Haber)
17	RAI 2	39	TRT Turk
18	RAI 3	40	CNN Turk
19	Animal Planet	41	Haber Turk
20	Aljazeera	42	TGRT
21	Discovery Channel	43	TA3
22	Eurosport	44	PRO TV International

WPS014 - Secure Voice Service

Service ID: WPS014

Service Name: Secure Voice Service

Portfolio Group: Workplace Services

Service Description: The Secure Voice Service is a voice collaboration service that provides user with the ability to collaborate and communicate through audio and audio/video in a secure network environment. The Service enables communication to other Voice Secure Domains outside of NATO VoSIP network (e.g. BICES).

Value Proposition: The Service enables real-time secure communication between more parties. This dramatically increases the effectiveness of the Command and Control and provides additional flexibility and efficiency to it, by saving time and cos of usually required travel.

Service Features: Secure Calls, Secure Video Calls, Secure Conferencing Calls, Secure Video Conferencing Calls, Hunt Groups, Pick Up Groups, Call Forwarding, and Extension Mobility Service are provided on the available NATO security domains.

Service Flavours:

Desk phone (Voice): provides a static IP desk phone and a number assigned in locations where the service can be installed (depending on the local infrastructure). The voice subscription is not part of the service.

Desk phone (Voice/Video): provides a static IP desk phone with additional video capability and a number assigned in location where the service can be installed (depending on the local infrastructure). The voice subscription is not part of the service.

Mobile phone (Voice): provides a mobile ability to collaborate and communicate through audio in a secure network environment. The voice subscription is not part of the service.

B2B Voice (Business to Business) provides NATO users the possibility to communicate through audio and video with external Voice networks such as Nations, Missions, Deployed CIS, NGO's and GO's.

Available on:

NATO Secret

Mission Secret

Service Prerequisites:

INF001 - LAN Service

INF014 - Transmission Service

SEC011 - Gateway Security Service (To Secure Domains outside NATO VoSIP Network)

Standard Service Support Levels:

Service Availability[1] Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device. For the price information per flavour, see the Service Rates document.

WPS015 - Voice Loop Service

Service ID: WPS015

Service Name: Voice Loop Service

Portfolio Group: Workplace Services

Service Description: The Voice Loop Service provides the user with the ability to communicate with a group of users through audio.

Value Proposition: Voice Loop Services allow easy communication between more than one party (CAOC's and CRC's). This increases reliability, flexibility and response time to Static Air Defence Centre mission of Air and Controlling Policing over NATO North and South Region.

Service Features: The Service allows the user to participate in different Conferences (Voice Loops) established with different locations with the ability of IP Voice recording.

> **Voice Loop Conferences:** Voice Loop provide to the user the ability to participate in a permanent open conference with all the participants in a specific region.
>
> **Voice Recording:** Allows IP Voice capture and preservation system, therefore constant recording of all Voice Loop voice content

Service Flavours: The Service is available as a single flavour.

Available on:

> NATO Unclassified

Service Prerequisites:

> For IP Phone: INF001 - LAN Service
>
> For Networking: INF005 - Infrastructure Networking Service
>
> For Communication: INF014 - Transmission Service

Standard Service Support Levels:

> **Service Availability**[1] **Target:** 99.5%
>
> **Service Restoration:** Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
>
> **N.B.** Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INFRASTRUCTURE SERVICES

V3.4

This page is left blank intentionally

INF001 - LAN Service

Service ID: INF001

Service Name: LAN Services

Portfolio Group: Infrastructure Service

Service Description: The LAN service provides users with local network connectivity. The LAN service is crucial to enable collaboration and communication. The LAN service is provided as a cabled infrastructure for all networks and as a wireless infrastructure for accessing only the unclassified and restricted networks.

Value Proposition: The LAN Service is a vital component enabling all local users to connect to the wider network. It is the key enabler for accessing all NATO customer facing Services such as Voice and Video, as well as Internet, and enabling services such as security and management. LAN services allow all entitled users to access shared NATO services and data across the NATO Enterprise.

Wi-Fi connections provide additional flexibility, allowing users to connect to the network from anywhere within the relevant Wi-Fi footprint, preventing users from being 'tied' to their desks.

Service Features: LAN Services are available on the NATO Security domains in wired and, in selected locations, as Wireless (Wi-Fi) configurations. The LAN Service will be capacity sized to support the number of connected devices and Users. This is with the understanding that all equipment is located within the same building and that the cabling system is available.

Service Flavours: The LAN Service is available in the following flavours:

Wired – This service flavour provides a physical connection to terminate and connect devices to one of the NATO networks.

By utilising NCIA deployed LAN Services, users are able to operate on all wired NATO networks including, but not limited to:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret (when invoked)

Wireless - This service flavour provides the ability to connect a specific client device to a network wirelessly.

By utilising NCIA deployed LAN Services, users are able to operate on all wireless NATO networks including:

NATO Unclassified

Available on:

NATO Unclassified
NATO Restricted – only wired
NATO Secret – only wired
Mission Secret (when invoked) – only wired

Service Prerequisites:

INF002 – NATO Network Point of Presence (PoP) service

Standard Service Support Levels:

	Availability[1] Target	Service Restoration Period
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

While this provides a standard availability target for the service, regional support arrangements and therefore the availability targets may vary and should be agreed during the SLA discussions.

Service Cost / Price: The unit of measure for the Service is Per Port, with 24 ports being minimum quantity and additional requests added in increments of 24 ports. For the price details, see the Service Rates document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF002 - NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service

Service ID: INF002

Service Name: NATO General Purpose Communication System (NGCS) Point of Presence (POP) Service

Portfolio Group: Infrastructure Services

Service Description: The NGCS POP Service primarily provides the infrastructure at points between communicating entities, where a connection is required. The NATO Network POP Service is defined as the provision of the infrastructure assets, capacity provisioning, and cyber security management elements that enable the user to establish any-to-any connectivity between connected networks.

Value Proposition: The NGCS POP Service is an integral component in enabling users to connect and collaborate between each other in support of the majority of NATO business activities and processes.

Service Features: The NGCS POP Services are available across all NATO Security Domains. NGCS POP Services feature the WAN Infrastructure Assets (Protected Core Access equipment in line with the valid Technical Architecture) and Cyber Security Management (layered security present at connectivity access points).

Service Flavours: The NGCS POP Service is available in the following flavours, although the exact details of each flavour will be subject to review as equipment and suppliers vary:

- **Pico POP** – This provides the termination of medium bandwidth transmission service (up to 100 Mbit/s links). Pico POP services are also required to support user communities up to 100 users.
- **Medium POP** – This provides the termination of medium bandwidth transmission services (100 Mbit/s up to 1 Gbit/s links). Medium POP services are required to support user communities of 100 to 400 users.
- **Large POP –** This provides the termination of high bandwidth transmission service (1 and 10 Gbit/s links). Large POP services are required to support user communities greater than 400 users.
- **Remote extension (Legacy)** – This provides the termination of small bandwidth transmission services (less than 100Mbit/s links). Remote extension services are also required to support up to 100 users. Considered as a connection for all legacy connections not meeting target architecture requirements. The service is available for static and deployable extensions.

Medium and Large PoPs are extendable/may be enhanced with the following gateways:

- **NATO to Nation Gateway (NNG):** The NATO to Nation Gateway is an agreed hand over point between NATO and a Nation to allow information exchange for AIS (static) services. NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NNG to the required location within the Nation. The NNG can be used for NU and NS (future NR) and offers the option to include V2 services (SBC required). Additional security (i.e. firewalls on both sides) is required.
- **Network Interconnection Point (NIP):** A Network Interconnection Point is an agreed hand over take over point (Federated Mission Network compliant) between NATO and a Nation to allow information exchange for NRF, Exercises and Missions (this includes ships). NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NIP to the required location within the Nation. The NIP

can be used for (NRF) NU, (NRF) NR and (NRF) NS and offers the option to include V2 services (SBC required).

Available on:

NATO Secret
NATO Restricted
NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Availability for NGCS POP Services is determined annually and is dependent upon enabling services and regional support arrangements. Availability target provided above is for 24/7 service, where the service option only in support hours will provide lower availability, to be agreed with the customer on the SLAs.

Service Cost / Price: The unit of measure for the Service is Per Instance. For the price details, see the Service Rate document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF003 - Enterprise Internet Access Service

Service ID: INF003

Service Name: Internet Access Service

Portfolio Group: Infrastructure Services

Service Description: Enterprise Internet Access Service comprises of the provision and supply of secure web browsing connectivity to the internet, mail relay and mail security sanitation. Additionally this service supports collaboration and interoperability amongst any dependent NATO resources.

Value Proposition: Enterprise Internet Access Service offers the user the access to the internet, enabling the user to conduct open source intelligence gathering, administration, welfare and many other activities to support their business needs. Wireless access has the additional benefit of allowing mobility in the working environment.

Service Features:

- Downstream bit rates
- Upstream bit rates
- Monitoring from our Network Operations Centre
- High-speed access
- Secure access
- Corporate Web Proxying
- Corporate Internet DNS Service

Service Flavours: The service is available in the following flavours:

- Fixed Internet Access: a fixed connection to the end user, by means of a cable, through which the user can access onto the internet.
- Wireless Internet Access: provision of wireless connectivity from the user's device to the internet.

Available on:

NATO Unclassified
NATO Restricted

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

	Availability[1] Target	**Restoration Period**
In support hours	**99.9 %**	**1 hour**
Out of support hours	**99.5 %**	**4 hours**

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF004 - Infrastructure Hosting Service

Service ID: INF004

Service Name: Infrastructure Hosting Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Hosting services offering provides standard virtualized and physical operating platforms to securely host applications on the required hosting environment. NCI Agency utilizes advanced server virtualization technologies, strict standards, and economies of scale to enable rapid delivery of cost-effective, fully-managed operating platforms with expanded, inheritable and NATO recommended security controls.

Value Proposition: Infrastructure Hosting Service offers the user multiple benefits; comprising of:

- Scalability; ensuring resource is available as and when the Hosting Application or Application Service needs it, ensuring no delays in the in expanding capacity or the wastage of unused capacity
- Lower Total Cost of Ownership (TCO) of the virtual infrastructure hosting is provided through a Shared Infrastructure model
- Location Independence; Application or Application Service can be assessed from any location with LAN connectivity
- Physical Security; physical security afforded to the servers which are hosted within a secure environment
- No Single Point of Failure; if one service fails the broader service can remain unaffected, ensuring service availability and reliability

Service Features: The Infrastructure Hosting Service offers the user the following:

- Fully managed operating platform infrastructure
    - State-of-the-art server hardware
    - Standardized operating systems
    - Redundant server hardware
    - Periodic technology refresh
- Full platform administration services
    - Server configuration
    - OS installation
    - OS upgrades and patching
    - Security hardening per NATO NOS standards
    - User management and audit log review
    - Virus protection and vulnerability mitigation
    - Disaster recovery support
    - Incident and problem resolution
- Monitoring features that include:
    - Hardware monitoring service
    - QoS measurement service
    - Performance measurement service
    - Reporting (availability, health and trend analysis)
    - Proactive monitoring
    - Cloud / hybrid monitoring and performance analytics service
- Configuration management features:

- OS deployment service
- OS Software update management service
- Asset and software reporting service
- Asset intelligence
- Compliance and settings management service

- Optional high availability and network load balancing of infrastructure hosting to ensure availability
- Optional Additional SAN/NAS disk storage as required
- Optional Backup/Archive services as required
- Capacity provisioning through scalable and flexible management of available resources

Service Flavours:

Physical General Purpose Server: A physical server comprising of a dual x86 CPU, 16GB RAM and 80GB 1 Disk storage.

Physical High Performance Server: A physical server comprising of a dual x86, 64GB RAM, 80GB 1 Disk Storage, dual 10GB network interface and SAN HBA.

Virtual Large Server: A virtual server supporting 8 vCPU's, 64GB RAM and 80GB disk storage, shared 10 gigabit network access.

Virtual medium Server: A virtual server supporting 4 vCPU's, 32GB RAM and 80GB disk storage, shared 10 gigabit network access.

Virtual small Server: A virtual server supporting 2 vCPU's, 8GB RAM and 80GB disk storage, shared 1 Gigabit network access.

All servers can be loaded with a Windows or Linux Operating system; have pre-installed anti-virus and malware protections. As part of the provisioning, all servers are hardened based on the NATO security policies.

The service flavours are also available with additional options:

- Redundancy – depending on the selected infrastructure flavour, redundancy capacity is provisioned to support the required availability. Physical server redundancy is provided through clustering or data replication.
- Load balancing for selected applications and protocols (e.g. HTTP) through the network infrastructure service (INF005)
- Additional SAN/NAS storage (INF007) – additional storage for the server instance to store user and/or application data.
- Backup/archiving – (INF016)

Available on:

NATO SECRET
MISSION SECRET
NATO RESTRICTED
NATO UNCLASSIFIED
Public Internet Access (PIA) Gateway

Service Prerequisites:

None

Standard Service Support Levels:

	Service Flavour	Availability[1] target during support hours	Availability target out of support hours
Level 1	Virtual Servers	99.9%	99.5%
Level 2	Physical servers with redundancy option	99.5%	99.0%
Level 3	Physical Servers	98.0%	98.0%
	Service Flavour	**Restoration period during support hours**	**Restoration period out of support hours**
Level 1	Virtual Servers	1 hour	4 hours
Level 2	Physical servers with redundancy option	4 hours	4 hours
Level 3	Physical Servers	4 hours	4hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF005 - Infrastructure Network Service

Service ID: INF005

Service Name: Infrastructure Network Service

Portfolio Group: Infrastructure Services

Service Description: The infrastructure network service provides the underlying infrastructure network services that are required to have a working IT environment. It provides essential services like Name resolution (DNS), dynamic IP address assignment (DHCP), time services (NTP), directory services (Active Directory). Additionally, the service incorporates the remote access infrastructure for the mobility of applicable Managed Devices. The service also provides optional load balancing and network acceleration for applications.

Value Proposition: The infrastructure network service is essential for a proper functioning IT environment. It provides customers the core network services that are required to use any other applications or collaboration tools.

Service Features:

- Domain Name Resolutions (DNS)
- Dynamic IP allocations (DHCP)
- Directory Services (Active Directory)
- Network time services (NTP)
- Network Access Control (NAC)
- Remote Access (Mobility) infrastructure
- Optional Load balancing for specific applications
- Optional network acceleration for specific applications

Service Flavours: The service is available as a single flavour, with the following additional options:

- Load balancing for selected applications and protocols (e.g. HTTP)
- Network acceleration for specific applications

Available on:

NATO SECRET
NATO RESTRICTED
NATO UNCLASSIFIED
MISSION SECRET
Public Internet Access (PIA)

Service Prerequisites:

None

Standard Service Support Levels:

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF006 - NATO Enterprise Directory Service (NEDS)

Service ID: INF006

Service Name: NATO Enterprise Directory Service (NEDS)

Portfolio Group: Infrastructure Services

Service Description: The NATO Enterprise Directory Service provides the capability to share trusted identity information between different systems and to Enterprise users. The information on identities (e.g. people, organizations, and devices) is retrieved from different, authoritative sources (e.g. APMS). NEDS covers the whole enterprise (including NATO HQ) and will become the standard way to exchange identity information across NATO. Information can be synchronised between different affiliate systems and automated workflows can be created, including provisioning and de-provisioning of User Accounts. NEDS service information can be made available through either the NEDS native interface or through customized interfaces such as Web Access, file based interface or SQL access.

Value Proposition: NEDS provides value to customers through the sharing of identity information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. This ensures a coherent set of identity data from authoritative sources, while increasing the security posture of the NATO Enterprise.

Service Features:

Identity Management – through shared information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. Information can be synchronised between different affiliates, and automated workflows can be created, including provisioning and de-provisioning of User Accounts. This increases the security posture of the NATO Enterprise, while ensuring a coherent set of identity data from authoritative sources.

Data sources/consumers can make use of the NEDS native interface for retrieving or updating identity information using LDAP(S). Otherwise tailored interfaces can be developed based on for instance SQL or file based connectivity.

Currently Affiliated Systems:

- **Automated Personnel Management System (APMS)** - provides a manpower and personnel database for all users at every level within the NATO Command Structure (Bi-SC).
- **Bi-SC AIS Active Directory** – provides existing NS accounts and receives NEDS automatically created accounts for new NATO Staff users (originating from APMS) and updated existing NS accounts when APMS information changes for a NATO Staff user.
- **NATO Network Control System** (**NNCS) Database** – provides Formal Military Messaging (ACP 127) information related to Address Indicator Groups (AIGs), Signal Message Addressee (SMAs) / Plain Language Addressee (PLAs) and Routing Indicators (RIs) as well as NATO Subject Indicator Codes (SICs).

The affiliate administrator (AA) (customer of the identity management feature) of a subscribing affiliate can choose from available authoritative attributes what he / she can receive. If the AA needs additional attributes currently not contained in NEDS than NEDS can connect to an additional authoritative affiliate (if identified and available) and the AA can subscribe to these new attributes.

White and Yellow pages - For an end-user, NEDS provides search and browse functions through a web browser to access information (e.g. name, telephone number, email-address, and room number). As the functionality of the application is increased, this interface will also provide additional features, such as access request submission/approval and self-service updates.

Access to Web Portal by NATO Staff users is provided using HTTPS.

Service Flavours: The Service is available as a single flavour, with the following options:

White and Yellow pages - This web application provides the capability to search and browse for published information on identities from affiliated systems. It is accessed through a standard web browser and available to all customer staff.

Identity Management: On the identity management side, the affiliate administrator (AA) (customer of the identity management feature) of a subscribing affiliate can choose from available authoritative attributes what he / she can receive. If the AA needs additional attributes currently not contained in NEDS than NEDS can connect to an additional authoritative affiliate (if identified and available) and the AA can subscribe to these new attributes.

Available on:

NATO Secret

In the future, instances of the service will also be available on the NATO RESTRICTED/NATO UNCLASSIFIED environment.

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF007 - Infrastructure Storage Service

Service ID: INF007

Service Name: Infrastructure Storage Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Storage Service, provides the user with data storage capacity in support of applications, user and system data. The infrastructure storage service offers different storage tiers to best suit the business requirements. The infrastructure storage service is accessible through SAN or NAS environment.

Value Proposition: Infrastructure Storage Service offers the user a more available and agile storage of data.

Service Features: The Infrastructure Storage Service is comprised of the following features:

- Enterprise-class (virtualized) disk storage controllers that provide high scalability, performance and availability.
- Highly available, redundant storage infrastructure with optional data replication, migration and backup features.
- NAS Storage infrastructure supports both NFS and CIFS file sharing.
- SAN storage infrastructure supports both FC and ISCSI connectivity.
- Redundant SAN architecture
  - Dual-fabric architecture
  - Enterprise-class directors and switches
- Highly-available NAS infrastructure
  - Utilizes same virtualized disk architecture
  - Supports both NFS and CIFS file sharing
  - Robust data snapshot/replication technology
- Security of data provided through management of access rights
- Optional local and remote data replication

Service Flavours:

- Storage Area Network (SAN) or
- Network Attached Storage (NAS).

Tier	Disk type	Target systems	NAS	SAN	Optional Replication
Tier 0	SSD	System Images	x	x	YES
Tier 1	Fiber 15K	Performance sensitive applications (e.g. DB's)	x	x	YES
Tier 2	SAS 10K	Typical applications	x	x	YES
Tier 3	SATA	Archiving/Backup	x	x	YES

For each of these flavours, there is high availability option available (please see Service Support Levels).

Access Method requirements:

a. SAN

1. Dual attached Host Bus Adapters (HBA) required per host

a. HBA and firmware must be supported by storage vendor.

2. Storage Load balancing software required.

b. NAS

1. Fault Tolerant Network Connection

Note: The infrastructure Storage service does not include additional services such as backup, or disaster recovery – these have to be requested in addition.

Available on:

NATO SECRET
NATO RESTRICTED
NATO UNCLASSIFIED
MISSION SECRET
Public Internet Access (PIA) Gateway

Service Prerequisites:

None

Standard Service Support Levels:

	Availability[1] target during support hours	**Availability target out of support hours**	**Service Flavour**
Level 0	99.9%	99.5%	Tier 0-1-2-3 with High-availability option (Replication/Mirroring)
Level 1	99%	98.5%	Tier 0-1-2-3 without High-availability option (Replication/Mirroring)
	Restoration period during support hours	**Restoration period out of support hours**	**Service Flavour**
Level 0	1 hour	4 hours	Tier 0-1-2-3 with High-availability option (Replication/Mirroring)
Level 1	4 hours	4 hours	Tier 0-1-2-3 without High-availability option (Replication/Mirroring)

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF008 - DCIS - DragonFly Service

Service ID: INF008

Service Name: DragonFly Service

Portfolio Group: Infrastructure Services

Service Description: The DragonFly service provides a wide array of deployable Command and Control (C2) communication and information systems to deployed commands of the NATO high readiness Response Force (NRF). In line with the requirements of the rapid reaction forces, Dragonfly enables:

- Communication network between deployed NATO command units.
- Connection up to 126 staff
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communication with mission partnering Nations and non-governmental organisations.

Additionally, the DragonFly security architecture utilises information labelling (protective marking), content aware firewalls, encryption, Network Intrusion Detection System (NIDS), access control, Host Intrusion Protection System (HIPS), content filtering for NS/MS connectivity, device control, anti-virus/anti-malware and accounting/auditing.

Value Proposition: The Dragonfly Deployable Communications & Information Services provide the user:

- Modularity: DragonFly utilises a common Commercial off the Shelf (COTS) equipment pool. Discrete elements can be combined as required for the deployment scenario and equipment can be interchanged or upgraded without having to replace large bespoke modules.
- Scalablity: DragonFly is designed to be configurable from small Command and Control deployments through to a full DCIS deployment with 126 users. Communications and IS equipment are scaled commensurate with the information exchange requirements for a full NATO Response Force (NRF) deployment.
- Deployability: DragonFly is designed as a Roll-on/Roll-off solution by tactical air transport, such as C-130, as well as transportable by rail and sea. The target for DragonFly to be fully operational in theatre is within 72 hours of arrival on site, with a subset of priority services to be available within 48 hours. All equipment is integrated into ruggedized outdoor and indoor transit cases with the latter deployed in DragonFly provided Biological and Chemical (BC) proof tents or buildings of opportunity (BOO).
- Sustainability: A whole life cycle approach to availability, reliability and maintainability has been applied, ensuring DragonFly components are interchangeable, upgradable, reconfigurable and replaceable, and comply with common standards which minimise the training burden. Integrated Logistics Support (ILS), Reliability, Availability & Maintainability (RAM) and Training plans are in place considered to ensure that the processes, skills and facilities are available to maintain the DragonFly capability to the required readiness levels and performance parameters.
- Interoperability**:** In order to comply with different command structures, mission types and deployment durations, DragonFly provides interoperability within NATO fixed Headquarters (HQ), Nations forces, Governments and Non-Government Organisations through standards based interfaces and conformance to the NATO Federated Mission Network Interoperability Profile.

Service Features: Dragonfly Service provides the following key services in deployable environment:

- Network - Wide Area and Local Area Connectivity (INF001)
- Voice (WPS009)
- Secure Voice (WPS009)
- Video Teleconferencing (WPS010)
- Formal Messaging (APP029)
- Informal Mail (WPS004)
- FAX Services
- Shared Database (PLT006)
- Document Publishing - on SharePoint (PLT001)
- Web Services (INF003)
- Network Management System (INF005)
- Domain Name Services (INF005)
- Network Services Automated IP Allocation (INF005)
- Time Services (INF005)
- Microsoft Certificate Services (WPS003)
- File and Print Services (WPS007)
- Backup and Restore Services (INF016)
- Windows System Monitoring
- Authentication Services (INF005)
- Anti-virus and Anti-malware
- Workstation Access Controls
- Host Intrusion Protection System (HIPS)
- Security Event Auditing
- Software Distribution and Updates
- Web Proxy Services
- Ability to host Functional Services

CIS Assets: The DragonFly comprises of the following system elements:

- Micro Communications Module (uCOM)
- Micro Information Services Module (uISM)
- Intra Nodal Distribution System (INDS)
- Service Access Points (SAP)
- Interface Exchange Gateway (IEG-B and IEG-C)
- Element Network Manager (ENM)
- Integrated Network Management System (INMS)
- Interface to Nations Module (INM)
- Wireless Crypto Router (WICR)
- Break our Boxes (BoB).
- MS Core
- NS Core

Non-CIS Assets: Air Conditioning Units, Generators, BC Tent and Filters, Transit cases with shock mount and F.O. bulkheads.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.

- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators.

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is as provided above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF009 - DCIS - Limited Interim NATO Response Force (NRF) CIS-Expansion (LINC-E) Service

Service ID: INF009

Service Name: Limited Interim NATO Response Force (NRF) CIS-Expansion (LINC-E) Service

Portfolio Group: Infrastructure Services

Service Description: The Limited Interim NRF CIS – Expansion (LINC-E) is a deployable CIS that provides limited Command and Control (C2) Communication and Information Systems to deployed commands of the NRF. The LINC-E provides a Point of Presence service which enables the extension of CIS services to resolute locations in a high readiness and deployable form. LINC-E service is not intended for high intensity mission capabilities, but for deploying core CIS services such as secure voice, data, printing, internet, limited video and data storage in a high readiness scenario. Furthermore, it's not compliant with Minimum Military Requirements as it lacks BC, Environmental protection and Roll-on Roll-off capabilities. The LINC-E Point of Presence service can be configured to include Functional Area Services on request.

Value Proposition: LINC-E can be used as a basis for low intensity but high readiness CIS support, provided that compliance to Federation Mission Network (FMN) profiles are achieved. Additionally, the LINC-E deployments can also be interconnected to form a cluster to support a greater number of users split across geographically separate small and/or large HQs, where a small LINC-E HQ can support up to 30 active users and a large LINC-E HQ can support up to 126 active users.

Service Features: The standard LINC-E provides the following NCI Agency-provided CIS services in a deployable format:

- Managed Devices (Laptop),
- Voice communications over IP,
- Video teleconferencing (VTC),
- Email,
- Internet/ intranet Web browsing,
- Data transfer,
- Data / file storage,
- Printing/ scanning/ plotting Services

Service Flavours: The different flavours of the LINC-E service can be obtained by choosing a combination of choices from each of the 3 categories of options available:

1. **By number of users supported:**
   - **Large LINC-E HQ:** Capable of supporting 126 active users
   - **Small LINC-E HQ:** Capable of supporting 30 active users.
2. **By Functional Area Services Supported:**
   - **LINC-E without Functional Area Services**
   - **LINC-E with Functional Area Services:** It is to be agreed with the customer which FAS's are to be integrated.
3. **By the non-CIS:**

- **Standard Point of Presence (PoP) LINC-E:** In addition to standard CIS, it comprises of the following non-CIS: 3 Transport Vehicles, 3 Trailers, 1 Tent (with Furniture), 3 Power Generating Sets (PGS) and 3 Environment Control Unit (ECU).
- **Expanded Point of Presence (PoP) LINC-E:** In addition to standard CIS, it comprises of the following non-CIS: 4 Transport Vehicles, 4 Trailers, 1 Tent (with Furniture), 4 Power Generating Sets (PGS) and 4 Environment Control Unit (ECU).

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF010 - DCIS - Communications Gateway Shelters (CGS) Service

Service ID: INF010

Service Name: Communications Gateway Shelters (CGS) Service

Portfolio Group: Infrastructure Services

Service Description: The Communications Gateway Shelter (CGS) service is a Deployable CIS that comprises of a transportable system which provides CIS assets to a deployed Combined Joint Task Force (CJTF) as needed to support NATO Strategic Command and Control. In support of the IT tasks the CGS incorporates NATO Secret (NS) LAN, a Mission Secret (MS) LAN, NS-MS Gateway, a NATO Unclassified (NU) LAN and peripheral equipment. It can support a maximum of 510 user stations and 510 telephones per security domain.

CGS can extend, in particular, Allied Command Europe (ACE) Automated Command and Control Information System (ACCIS) services to deployed NATO Commands and connected users from/to the static NATO Commands. The CGS was assembled using components and shelters from DCIS Baseline PoPs and is currently assessed as operational, but not high intensity compliant. (The end of life of the CGS capability is assessed as 2018 and is considered as Assets Available until the end of 2018 with limited provision of core CIS services, but without provision of FAS and INM capabilities.)

Value Proposition: The CGS serves as one of the CJTF CIS key elements, as it will tie most of the other CJTF CIS systems together for interconnection. (The CGS is considered as mitigation for MJO1 scenarios until CP0A0149Rev1 Increment 2 assets will be available. CGS is currently used in support of NRF due to lack of other DCIS equipment.)

Service Features:

CIS Assets: The CGS comprises of the following system Servers:

- Gateway
- Management Server
- Primary Domain Controller
- Secondary Domain Controller
- E-mail Server
- Virtualization Server 01
- Virtualization Server 02
- Antivirus Server
- MS S/W Update Server

Non-CIS Assets:

- A two-axle Truck for the transportation of the CGS Shelter.
- The CGS Shelter can also be transported on any transport vehicle equipped with TWIST-locks for 20-ft ISO Containers. In addition to transportation on road, the system is designed for transportation by rail, cargo ship, and cargo aircraft.
- A power generator set (PG) comprising of two diesel generators (DG) mounted on a single-axle Truck.
- The CGS Shelter houses the LAN equipment, the operator stations and Support System comprising; air conditioning, biological/chemical (BC) protection and power distribution.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF012 - SATCOM Service

Service ID: INF012

Service Name: SATCOM Service

Portfolio Group: Infrastructure Services

Service Description: The SATCOM service provides bandwidth to remote customers unable to be supplied by terrestrial infrastructure. The SATCOM infrastructure provides state-of-the-art communications supporting deployed operations anywhere within NATO's area of responsibility. It does this with its own ground equipment and control systems, operating with satellite capacity leased from the national governments of Great Britain, France and Italy.

Value Proposition: SATCOM Service provides the following value and benefits:

- ***Location*:** SATCOM services allow the customer to extend their communications networks to anywhere within NATO's area of responsibility.
- ***Scale**:* The service is scalable to support a variety of different deployments in both size and complexity, ranging from one telephone circuit to a complete intra-theatre hub and spokes and backhaul to the static HQ.
- ***Redundancy:*** The static SATCOM infrastructure has no single point of failure.
- ***High Availability and Security:*** SATCOM uses a variety of methods to ensure that communications in a hostile electronic environment maintains a high level of availability and security. These methods include:
  - Frequency hopping modems
  - Hardened satellites
  - Beam-nulling satellite antennas
  - Beam-steering satellite antennas

Service Features:

- ***Redundant anchoring using dispersed locations:*** provides greater resilience and availability, plus space diversity.
- ***Dynamic bandwidth allocation*** using global QoS to set priorities. Links are transparent to NGCS network.
- ***Hardened satellites at X-band:*** increased ability to work in a hostile electromagnetic environment.
- ***Beam-nulling and beam-steering satellite antennas at X-band:*** increased ability to work in a hostile electromagnetic environment.
- ***Anti-jam modems:*** increased ability to work in a hostile electromagnetic environment.
- ***Voice and data services:*** Links are transparent to NGCS.
- ***Inherently secure communications*** through the use of closed networks and the ability to integrate with VPN, comsec and transsec services. Increases security and integrity of information.
- ***One-stop-shop*** for all satellite queries and issues: NATO's centre of excellence for all SATCOM matters.
- ***Fully managed communications suite*** from an organization that understands the needs of the military. Centralised management ensures continuity, efficiency and full systems visibility.

- ***Anchor station manning*****:** minimum one person on shift at all times to ensure timely response to faults, events and changing situations.
- ***Ability to react quickly to new requirements*** and changing circumstances: SATCOM is set up to process requirements within the SLA agreed with ACO.

Service Flavours:

1. ***Individual deployment:*** Small, commercial handheld and portable voice and low-speed data communications
2. ***Individual operational deployment:*** hand-held, vehicle and ship-mounted UHF systems providing secure, narrow-band voice and data.
3. ***Wideband deployment*****:** transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using X- or Ku-band satellites
4. ***Wideband secure deployment:*** transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using anti-jam modems and hardened X-band satellites

Additionally the table below provides infrastructure or support options available under each flavour, which cater to a variety of deployment requirements.

Service Flavour	Options under the Flavour	Description	in units	Support level available
Individual deployment	Inmarsat	Small, highly portable secure and insecure voice and data communications for initial deployments		
	Iridium	Handheld telephone-type communications		
Individual operational deployment	DAMA controller maintenance	This is the hub of the TACSAT DAMA system		2nd, 3rd line
	UHF TACSAT support	TACSAT radio 3rd-line repair and management	12 channels	3rd line
Wideband deployment	X-band anchoring	4 sites with 10 antennas to anchor all of NATO's broadband satellite communications, including anti-jam. Includes EMP assets.	300MHz	SAA production, 3rd line
	DCIS TSGT support	3rd-line maintenance, repair and upgrade management.	As requested	3rd line
	DCIS DSGT support	3rd-line maintenance, repair and upgrade management.	As requested	3rd line
Wideband secure deployment	SkyWAN operation and maintenance	Hub and spoke VSAT system, provided as VNC by LUX, currently used for NC2	2MHz, 8 terminals	2nd, 3rd line
	Melusina 2 administration	Administration of the LUX Ku-band VNC contribution	42MHz	3rd line
	DCIS TSGT support	3rd-line maintenance, repair and upgrade management	As requested	3rd line

	DCIS DSGT support	3rd-line maintenance, repair and upgrade management.	As requested	3rd line

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels:

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF013 - Very Low Frequency (VLF) Broadcast Service

Service ID: INF013

Service Name: Very Low Frequency (VLF) Broadcast Service

Portfolio Group: Infrastructure Services

Service Description: Very Low Frequency (VLF) Broadcast services provide Submarine Operating Authorities (SUBOPAUTH's) with robust, secure and timely message delivery within the NATO Area of Responsibility in order to ensure effective Command and Control of sub-surface forces.

Value Proposition: VLF is the primary means of communicating with submarines. The NCI Agency managed VLF network is a key enabler for connecting shore SUBOPAUTH's to VLF Broadcast Radiating Stations for subsequent message delivery to submarines. The service additionally includes Broadcast Control Station (BCS) equipment which provides a live picture of the network status including; site status, keystream delivery and clear indication of system issues. Coupled with the ability to pass remote Over the Air Monitoring to a distance site and connection to external networks, this makes the BCS system extremely flexible for conducting submarine operations across NATO.

Service Features:

- Broadcast Control Authority (BCA)
  - Provides broadcast traffic at Mission Secret
  - System Management
  - Hardware and Software solutions
  - Interfaces with crypto for secure communications
  - Interfaces with Message Handling Systems (MHS)
- Broadcast Control Station (BCS)
  - Live connectivity picture
  - Broadcast Traffic Table management
  - Connection to NATO provided Broadcast Radiating Station (BRS) via the VLF network or to national transmitters via external lines.
  - Fully Redundant
  - Swap and replace solution
  - Facility to pass remote OTAM between sites
  - Group CHAT facility
  - Minimum operator involvement
- Broadcast Radiating Station (BRS)
  - Passes broadcast traffic to national transmitters
  - Utilises same hardware and software as BCS
  - Fully Redundant
  - Swap and replace solution
  - Minimum operator involvement
- NATO VLF WAN
  - NCI Agency managed dedicated IP network for VLF BCS
- Broadcast Support Site (BSS)
  - Provides test bed for system changes
  - Training facility

Service Flavours: The Service is available as a single flavour, with the following options:

- Complete end to end provision of VLF services (i.e. MHS to end user) or
- Individual or a mixture of the features listed.

Available on:

Mission Secret
NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF014 - Transmission Service

Service ID: INF014

Service Name: Transmission Service

Portfolio Group: Infrastructure Services

Service Description: Transmission Services provide the transmission fabric, capacity management, service management and physical connectivity required by the Network Infrastructure Services to deliver any-to-any connectivity to users, with differentiated service levels. Transmission Services are delivered as managed capacity over wired or wireless transmissions bearers. The former can be local area, or wide area (e.g. leased lines, dark fibre). The latter are line of sight (LOS) links used for specific locations where wired connectivity is impossible. Transmission Services are defined by the attributes of the physical link, the capacity provisioning and monitoring mechanisms, and the physical and management interfaces presented to the Network Infrastructure Services. Transmission Services are largely outsourced to 3rd parties (Commercial Service Providers and/or National Defence Networks NDNs).

Value Proposition: Transmission Services underpin the NATO wide area network and provide the primary means by which all services and capabilities reach geographically dispersed users.

Service Features: Transmission Services provide high readiness transport links scaled to meet and exceed the traffic densities for all NATO nodes. Transmission Services ensures the effective transport of services and data across the NATO Enterprise by means of a Protected Core Network delivering all-encrypted traffic to their destinations.

Service Flavours: The Service is available in the following flavours:

Wired: Wired Transmission Services are normally delivered by fibre optic cabling as part of contract with a Telecommunications provider as a leased line. Links are procured by Capacity and Availability of the link. Available bandwidths:

- 100 MB
- 1 GB
- 10 GB

Wireless: Wireless Transmission flavours consist of links used to connect physically remote sites and come in the form of:

- Digital Line of Sight (DLOS): Consists of microwave radio transmission with directional antennas (2-34 Mbit/s) (Includes CIP-67, and only a static provision of the service; the deployable DLOS transmission service can be found separately in INF025);
- Satellite Communications (SATCOM): Due to the size and complexity of this flavour, it is provided as a separate service (INF012);
- High Frequency, Very High Frequency: Due to the size and complexity of this flavour, it is provided as a separate service (INF029);
- Very Low Frequency (VLF) Transmission: Due to the size and complexity of this flavour, it is provided as a separate service (INF013).

Available on:

NATO Unclassified
NATO Restricted
NATO Secret

Mission Secret (when invoked)

Service Prerequisites:

None

Standard Service Support Levels: Service Availability for Transmission Services is determined annually and is dependent upon enabling services and regional support arrangements.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF015 - Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD Service

Service ID: INF015

Service Name: Broadcast, Maritime Rear Link and Ship-Shore (BRASS) System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) Service

Portfolio Group: Infrastructure Services

Service Description: The NATO Broadcast, Maritime Rear Link and Ship-Shore (BRASS) system is designed to support all NATO Maritime missions. It provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks**.** The System Test Integration and Verification and Reference Maintenance Diagnostic (STIV-RMD) facility replicates a minimal and representative BRASS operational site, mirroring the hardware and software components used in the BRASS Initial Core Capability, to the extent possible, with minimal additional hardware and software modules. The service includes all functions necessary to test and validate all services performed in an operational BRASS node. It is principally used for maintenance, testing and verification of BRASS software and its future implementations and is installed at Casteau Mons (SHAPE, Belgium), in NCIA facilities. The system can also be used for hands-on training of NATO/national BRASS personnel. The STIV-RMD facility interfaces the NGCS (NATO General Communication System) to connect to NCIA radio sites in The Hague and Staelduinen (NLD). The service is built from two nodes. One representing the standard BRASS node and the second allowing the simulation of the traffic up to the HF modem level. It is equipped with standard crypto units that are used in BRASS nodes and can be used in the simulation chains with unclassified traffic and crypto keys.

Value Proposition: The BRASS STIV-RMD facility allows testing of the key-streams transmitted/received by radios at the NCIA sites (HF TX in Staelduinen and the HF RX radio site in The Hague) without engaging assets required for military operations. The service design allows the simulation of the traffic without the need to use full radio equipment chains. The BRASS STIV-RMD facility is built in a manner similar to an operational system. The system processes, stores and disseminated unclassified data only and doesn't perform real operational activity, which makes STIV RMD a perfect tool to perform hands-on training for the NATO and national BRASS personnel.

Service Features:

- The system includes all functions necessary to test and validate all services performed in an operational BRASS node such as:
- Management of NATO/national Broadcasts, Ship Shore, MRL, MATELO and Point-to-Point circuits (STANAG 4285, STANAG 5066);
- Management of crypto equipment;
- Automatic storage and retrieval of message traffic handled in the centre;
- Remote control of the assets belonging to the system (including radio devices, antennae and communication links)
- The system includes the necessary hardware capacity and the full set of software tools required to maintain the BRASS software

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 98.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF016 - Infrastructure Backup/Archive Service

Service ID: INF016

Service Name: Infrastructure Backup/Archive Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Backup/Archive Service provides the user with an automated and fully managed capability to copy business data, active and inactive, to a backup target such as a (virtual) disk or (virtual) tape. This services delivers a high-speed copy and restore functionality to minimize the risk and impact of failures, human errors or disasters that could potentially jeopardize business-critical data. Depending on the customer requirements, backups can be kept on-site or off-site. The backup service is delivered in conjunction with the file archiving capability which, in addition, provides the means to effectively manage data for retention and long-term access and retrieval. This capability is primarily focused on maintaining older or inactive data for extended periods of time. This service combines and applies both backup and archival in order to optimize the cost and improve the overall effectiveness of the NCI-Agency storage infrastructure. Backup is more efficient in an environment that has an effective archiving solution. Both capabilities will therefore be offered in one service.

Value Proposition: The Infrastructure Backup/Archive Service:

- Provides the ability to meet regulatory and legal requirements.
- Enables the storage of large amounts of historic data.
- Improves the ability to recover from a disaster.
- Data Archival facilitates shorter backups and reduces primary storage needs, thus diminishing total operating costs.
- Reduced risk of losing critical data.
- Facilitates business continuity.

Service Features:

- Fully managed and automated data protection and archive solutions.
- Enterprise-class virtual tape technology; highly scalable and performant.
- Automated real tape technology (high capacity tape drives and automated tape libraries)
- Fully secured data access
- Disaster recovery support

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Public Internet Access (PIA) Gateway

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF017 - DCIS - In-Theatre Mobile CIS Detachment (IMCD) Service

Service ID: INF017

Service Name: In-Theatre Mobile CIS Detachment (IMCD) Service

Portfolio Group: Infrastructure Services

Service Description: The In-Theatre Mobile CIS Detachment (IMCD) Service provides limited deployable Communication and Information Systems and has been extended from ISAF to serving other customer AOM and Exercise requirements. The IMCD service can be deployed in either vehicle-mounted shelters or ruggedized transit cases and can support up to 126 users. The infrastructure of IMCD is based on the LINC-E but is not designed to work in a clustered node configuration of small and large HQs, therefore it's not suitable for small exercises or operations where a single small PoP is sufficient, nor does it have the functionality to connect geographically separated deployments.

Value Proposition: IMCD is intended for low intensity but high readiness CIS support in deployed environments, provided that compliance to Federation Mission Network (FMN) profiles are achieved.

Service Features: The features of IMCD Service are:

CIS Assets: The IMCD provides the following NCI Agency-provided CIS services in a deployable format:

- Voice communications over IP,
- Video teleconferencing (VTC)l,
- Email,
- Internet/Intranet Web browsing,
- Data transfer,
- Data/ file storage,
- Printing/ scanning/ plotting services.

IMCD consists of the following SATCOM terminals:

- Dual Band Auto-Pointing Rapidly Deployable Terminal (DART)
- Bi-Band Satellite Suitcase Terminal (BBSST).

Non-CIS Assets: 3 CVRTs (type SHERPA), trailers, Power Generation Systems (PGS), and tents.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF018 - DCIS - Mini Point of Presence (Mini-PoP) Service

Service ID: INF018

Service Name: Mini Point of Presence (Mini-PoP) Service

Portfolio Group: Infrastructure Services

Service Description: The Mini Point of Presence (Mini-PoP) is a deployable CIS that provides limited Command and Control (C2) Communication and Information Systems to deployed commands of the NATO Response Force (NRF). The purpose of Mini-PoP service is extending CIS services to resolute locations for small teams in a high readiness, easily transportable and rapidly deployable form. Mini-PoP service is not intended for high intensity mission capabilities, but for deploying core[1] CIS services such as secure voice, data, printing, internet, limited video and data storage in a high readiness scenario. Mini-POP is interoperable with DragonFly.

Value Proposition: The Mini-PoP service is an easily deployable and transportable Mini Point of Presence solution for small teams and provides core CIS services. It can support 12 users (8 users in the transit case) and has roll-on/roll-off capability. The service also incorporates a small Dual band (X and Ku) Auto-pointing Rapidly Deployable SATCOM Terminal (DART) enabling Mini-PoP connectivity through SATCOM.

Service Features:

CIS Assets: The Mini-PoP provides the following NCI Agency-provided CIS services in a deployable format:

- Laptops,
- Crypto Devices,
- Voice over IP,
- Video teleconferencing,
- Email,
- Internet/intranet web browsing,
- Data transfer,
- Data/file storage,
- Printing/ scanning/ plotting Services,
- DART Terminal for SATCOM connectivity,
- Interoperability with the major NATO Response Force PoP (DragonFly).

Non-CIS Assets: UPS.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

[1] The services provided are detailed in the Service Features section.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF019 - DCIS - Theatre Liaison Kit (TLK/ILK) Service

Service ID: INF019

Service Name: Theatre Liaison Kit (TLK/ILK) Service

Portfolio Group: Infrastructure Services

Service Description: The Theatre Liaison Kit (TLK/ILK) Service provides handheld limited Command and Control (C2) Communication and Information Systems to deployed commands of the NATO high readiness Response Force (NRF). TLK/ILK Service includes a man portable secure CIS consisting of 2 transit cases (25 Kg per case) providing secure data, voice, video teleconferencing, email and printing capabilities for 4 users. It additionally includes Broadband Global Access Network (BGAN) and INMARSAT Handset as a Deployable CIS. The (former) ISAF Liaison Kit (ILK), originally built for ISAC, has been upgraded to provide the same functionality as the TLK. TLK/ILK is interoperable with DragonFly.

Value Proposition: TLK/ILK Service provides rapidly deployable, man portable CIS services for small teams (up to 4 users). It is designed as high readiness with Roll-on/Roll-off capability and is high intensity mission capable.

Service Features:

CIS Assets: The TLK/ILK provides the following NCI Agency-provided CIS services in a deployable format:

- Managed Devices (4 laptops)
- Voice communications
- Data communications
- Video teleconferencing,
- Email,
- Internet/Intranet Web browsing,
- Data transfer,
- Data/file storage,
- Printing/ scanning/ plotting Services
- Connectivity of up to 1Mbit provided through BGAN commercial SATCOM,
- IINMARSAT handsets

Non-CIS Assets: UPS.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF020 - DCIS - Deployable CIS Equipment Pool (DCEP) Service

Service ID: INF020

Service Name: Deployable CIS Equipment Pool (DCEP) Service

Portfolio Group: Infrastructure Services

Service Description: The Deployable CIS Equipment Pool (DCEP) assets consist of desk-top terminal equipment to provide communications and IT services to the deployed end user. This equipment includes classified and unclassified workstations, classified and unclassified telephones, projectors, multi-function devices (MFD), VTC terminals, multi-point voice conference devices, large screens and workstations with multi-screen capability.

Value Proposition: DCEP equipment readiness is actively managed and sustained in a manner that ensures equipment availability to perform the mission within prescribed timelines. This service includes pre-configuration and delivery of DCEP equipment to the operational location in the Mission-Ready State.

Service Features:

CIS Assets: The DCEP provides the following NCI Agency-provided CIS services in a deployable format:

- Managed Devices (Desktop and laptop)
- Windows and COMSEC Licenses
- Scanners
- Switches
- Printers
- Monitors
- VoIP phones
- Projectors/Beamers
- Handheld Radios
- VTC Equipment

Non-CIS Assets: None.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF021 - DCIS - Third Generation Transportable Satellite Ground Terminal (TSGT) and Upgraded Transportable Satellite Ground Terminal (UTSGT) Service

Service ID: INF022

Service Name: Third Generation Transportable Satellite Ground Terminal (TSGT) and Upgraded Transportable Satellite Ground Terminal (UTSGT) Service

Portfolio Group: Infrastructure Services

Service Description: The Service provides a Deployable CIS to deployed commands of the NATO high readiness Response Force (NRF). It is designed to support up to 126 staff and enable them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission partnering Nations and non-governmental organisations.

Each of the 3rd Generation and Upgraded TSGT systems can provide up to 8Mb of multi-carrier satellite bandwidth.

Value Proposition: The Service extends C2 Services worldwide, thus enabling Operational Commanders to execute NATO Council Approved Operations worldwide.

Service Features:

CIS Assets: The 3rd Generation Transportable Satellite Ground Terminal (TSGT3G) and Upgraded Transportable Satellite Ground Terminal (UTSGT);

Non-CIS Assets: Power Generation System (UTSGT only), Shelters, AIRCO System (ECU), BC System.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours:

TSGT3G - T1 Variant: equipped with a 4.6 meter antenna and a 750W power amplifier, as well as a 2.4 meter pop-up antenna with a 250W power amplifier, with options to use one of them, but not simultaneously.
TSGT3G - T2 Variant: equipped with the 2.4 meter pop-up antenna and 250W power amplifier.

Upgraded TSGT (UTSGT): provides X-Band SATCOM Bandwidth, and entails SHF SATCOM TSGT, 3rd Generation T2 terminal, Antenna TSGT, 3rd Generation T1 Terminal and 3rd Generation TSGT Generator (Non-CIS).

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is as provided above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF022 - DCIS - Deployable Satellite Ground Terminal (DSGT) Service

Service ID: INF022

Service Name: Deployable Satellite Ground Terminal (DSGT) Service

Portfolio Group: Infrastructure Services

Service Description: The Deployable Satellite Ground Terminal (DSGT) Service is a Deployable CIS that provides Communication and Information Systems to deployed commands of the NATO high readiness Response Force (NRF). The requirements of the rapid reaction forces require a capability to support up to 126 staff and enable them to:

- Communicate between deployed NATO command units;
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS);
- Communicate with mission-partnering Nations and non-governmental organisations;

Value Proposition: The Service extends C2 Services worldwide, thus enabling Operational Commanders to execute NATO Council Approved Operations worldwide.

Service Features: DSGT Service provides X-Band SATCOM Bandwidth.

CIS Assets: The 1st and 2nd Generation Deployable Transportable Satellite Ground Terminal (DSGT), includes System Engineer PC/Laptops;

Non-CIS Assets: UPS, Transit Cases,

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours:

1st Generation DSGT: The 1st Generation DGST consists of a 2.4 meter X-band providing a Limited Interim NRF CIS (LINC).
2nd Generation DSGT: The 2nd Generation DGST, with a 2.4 meter X-band antenna and featuring an upgraded 200 watt power amplifier, provides a Limited Interim NATO Response Force Communications and Information System Expansion Capability (LINC-E).

Available on:

NATO Unclassified
NATO Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF023 - Network Services Fulfilment (NSF) Service

Service ID: INF023

Service Name: Network Services Fulfilment (NSF) Service

Portfolio Group: Infrastructure Services

Service Description: Network Service Fulfilment (NSF) is a service to manage provisioning and delivery of the network services, encompassing lifecycle stages from requesting the network services until their retirement in an orderly and well-defined fashion. The NSF process streamlines and tracks all the essential network service-provisioning activities such as; requesting, funding/eligibility validation, design, configuration management, implementation, testing, security accreditation and service operation. The Service relies upon funding/eligibility, SLA/CSLA, security accreditation, logistics, and engineering (implementation and O&M) processes

Value Proposition: The NSF Service enhances the network services provisioning by:

- maintaining user and customer satisfaction through efficient and professional handling of all network service requests,
- providing the means for users to request and receive authorized, qualified and validated network services,
- providing a single point of contact for information to users and customers about the availability of services and the procedure to obtain them,
- providing visibility and information to service implementation, operation communities.

Service Features: Currently, the NSF Service is provided by use of three software tools, namely SRTS, CAST and DCIS. However, the SRTS and DCIS tools are to be replaced in 2017, with an ITSM based solution.

Service Flavours:

Duration related flavours:

- Permanent network services (duration 1 year or longer)
- Temporary network services (finite duration, less than 1 year)
- Contingency network services (Hybrid of the two above, normally used for deployable network services for ops/ex. These services are to be requested once initially and then requested to be activated/deactivated for finite durations thereafter).

Urgency related flavours:

- Urgent/priority (mostly used for operational needs, processed within 5 working days)
- Routine (processed within 25 working days)

Complexity related flavours:

- Simple (less than 5 network segments)
- Medium (6-30 network segments)
- Complex size (31+ network segments)

Available on:

NATO Unclassified
NATO Restricted
Mission Secret

NATO Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF024 - DCIS - High Frequency (HF) Service

Service ID: INF024

Service Name: Deployable Communications & Information Systems (DCIS) - High Frequency (HF) Service

Portfolio Group: Infrastructure Services

Service Description: The DCIS High Frequency Service with all ancillaries is a Deployable CIS Service that provides High Frequency Command and Control (C2) Communication and Information Systems to deployed commands of the NATO high readiness Response Force (NRF). The requirements of the rapid reaction forces require a capability to support up to 126 staff and enable them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission-partnering Nations and non-governmental organisations.

Value Proposition: The DCIS High Frequency (HF) Service is capable of providing secure voice and secure data capability in the 3-30MHz range.

Service Features: The features of the DCIS High Frequency Service is:

CIS Assets: The HF Service provides the following NCI Agency-provided CIS services in a deployable format:

- HF Radio Systems,
- Ancillaries,
- Laptops,
- Printers.

Non-CIS Assets: BC Shelter, UPS, Power Assembly, Generators, Lifting device

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF025 - DCIS - Deployable Line of Sight (DLOS) Service

Service ID: INF025

Service Name: Deployable Communications & Information Systems (DCIS) – Deployable Line of Sight (DLOS) Service

Portfolio Group: Infrastructure Services

Service Description: The DCIS Deployable Line of Sight (DLOS) (Short Range and Long Range) Services is a Deployable CIS that provides limited Command and Control (C2) Communication and Information Systems to deployed commands of the NATO high readiness Response Force (NRF). The requirements of the rapid reaction forces require a capability to support up to 126 staff and enable them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission partnering Nations and non-governmental organisations.

Long Range Line of Sight (LRLOS) system provides two full-duplex LRLOS links, each system consists of one Biological - Chemical (BC) protected shelter mounted on a PFE vehicle.

The Short Range Line of Sight (SRLOS) system provides four full-duplex SRLOS links each system consists of one (BC) protected shelter mounted on a PFE vehicle.

Value Proposition: Following modification of the systems in 2015:

- The LRLOS system is capable of establishing an 8 Mbps Ethernet Link over a distance up to 50 kilometres. The shelters will support independent 8 Mbps links. This link can be used to extend the NATO network for deployed user groups.
- The SRLOS system is capable of establishing an 8 Mbps Ethernet Link over a distance up to 30 kilometres. The shelters will support independent 8 Mbps links. This link can be used to extend the NATO network for deployed user groups.

Service Features:

CIS Assets: The DLOS Service provides the following NCI Agency-provided CIS services in a deployable format:

- Laptop,
- Fibre Optic System,
- Switch,
- Modem,
- FOMUX
- Transceiver,
- Mast,
- Self-Aligning Antenna,

Non-CIS Assets: BC-Shelter, UPS, Lifting device, Power Assembly, Generators.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours:

1. Long Range Line of Sight (LRLOS) system
2. Short Range Line of Sight (SRLOS) system

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF026 - DCIS - Deployed Forces Operational Gateway (DOG) Service

Service ID: INF026

Service Name: Deployed Forces Operational Gateway (DOG) Service

Portfolio Group: Infrastructure Services

Service Description: The Deployed Forces Operational Gateway (DOG) is the CIS service anchor point for all NATO Deployed Forces that interface into the NATO General-purpose Communications System (NGCS) static CIS network. The deployed forces in NATO operate primarily in the mission secret domain (MS) whilst the NATO core network primarily operates in the NATO Secret domain (NS). As NATO increased its level of ambition for deployed operations, the requirement of cross domain connectivity was identified between MS and NS, as well as between different MS domains. The Information Exchange Gateway (IEG) service facilitates this functionality, with IEG-C being the gateway that interfaces MS and NS domains. The IEG-C was deployed into SHAPE in 2004 to interface ISAF and Balkan MS domains with NS; where SHAPE is known as the NATO DOG (NDOG). With the inception of the NRF concept, a requirement for additional NRF gateways had been identified. The NATO Response Force gateways, including the IEG–C capability, were implemented at the static Satellite Ground Terminals identified to support the NRF missions, SGT F05, Norway and Castlegate in Germany. These sites are known as the NRF Mission DOGs (MDOGs).

Value Proposition: Mission DOGs enable to enhance Satellite payload, avoid terrestrial network limitations and to provide redundancy. There is an on-going review of these current locations in order to optimize the performance of the DOG.

Service Features: The DOG capability has been recognized as an essential component in the NATO inventory. Each DOG consists of the following elements:

- Terrestrial network connectivity into NGCS and the respective NS, MS and NU domains,
- Satellite Connectivity -
- NDOG has BGAN network interconnectivity with Inmarsat,
- MDOGs have X Band Satellite connectivity through the SGT terminal with each MDOG able to provide connectivity for 12 deployed TSGTs,
- An IEG-C for cross domain service flows,
- Cross domain Service interfaces for Mail, Voice and VTC.

CIS Assets: the DOG Service provides the following NCI Agency-provided CIS services in a deployable format:

NDOG:

- Routers 38xx series with software support
- Switches
- Firewalls
- VX 900
- Voice Gateway and Call Managers
- Crypto Equipment

MDOG:

- Crypto Equipment

- Servers
- Switches
- VX 900
- Voice Gateway and Call Managers
- Firewalls
- Routers 38xx series with software support

Non-CIS Assets: None

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours:

1. NATO Domain NDOG
2. Mission Domain MDOG

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is per anchor site. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF027 - DCIS - Mission Preparation Centre Service

Service ID: INF027

Service Name: Mission Preparation Centre – Deployable Communications & Information Systems (DCIS) Service

Portfolio Group: Infrastructure Services

Service Description: The **Mission Preparation Centre** (MPC) is a Deployable CIS service, also known as PoP Replication Centre (PRC), provided by NCI Agency. The MPC is an In-Garrison capability to connect DCIS PoP equipment in the Static Domain to the Deployed Mission Secret (MS) Domain network.

The NATO Static AIS Domain and NATO Deployed Domain are protected by a Firewall, the Mission Anchor Point Deployed-Forces Operational Gateway (DOG) acts as the conduit between these domains. The MPC is dependent on the DOG Service, therefore the DOG Service must be in place in order to successfully implement the MPC Service.

For DCIS equipment on short Notice to Move (NTM), e.g. DCIS assets assigned to NRF in stand-by, the Community of Interest (COI) enabling and COl services must also be installed and operational. This is necessary to support the generic Command Control (C2) service requirements of the Joint Task Force (JTF) or Land Component Command (LCC) HQ that the specific DCIS PoP will support upon deployment. Additionally, all applicable Information Assurance tools and processes shall be activated.

Value Proposition: The Service provides capability to connect in-garrison (Static CIS) PoPs (and all ancillary CIS) to the NATO/NCIA Deployable Mission Domain. Enabling the distribution of Mission specific configuration updates, system patches, security patches and updates and also supports on-the-job training of Customer personnel.

Service Features:

CIS Assets: Server Hardware, Engineer Laptop, Printers/ MFDs.

Non-CIS Assets: None.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

The Mission Preparation Centre serves as an In-garrison Replication Centre for equipment preparation and updating prior to deployment. The Mission Preparation Centre has:

- The appropriate security certification for storage and use of cryptographic equipment and key material,
- connection to the NGCS Protected Core Segment which allows interconnection with the NGCS Gateways, deployed nodes and the NCI Agency Network Control Centre, and

- sufficient test equipment to simulate other Nations' networks.

The MPC Service includes Preventive Maintenance (PMI) and Corrective Maintenance (CMI) at Level 3 of the MPC network and information system hardware, shipping costs (3 locations) to/from repair facility, and supply of Level 1 through Level 3 system spare parts and consumables.

In support of the DCIS mission preparation, the NCI Agency will conduct overall management of all services through their appropriate Network Management/Operations Centre, while the Customer's Deployable Communication Module (DCM) personnel will perform local O&M activities in support of the Provider.

Service Flavours: The Service is available as a single flavor.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Mission Anchor Point Deployed-Forces Operational Gateway (DOG) Services.

Standard Service Support Levels:

Service Availability[1] Target: 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is as provided above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF028 - ACCS Sensor Integration Module (ASIM) Service

Service ID: INF028

Service Name: ACCS Sensor Integration Module (ASIM) Service

Portfolio Group: Infrastructure Services

Service Description: The ACCS Sensor Integration Module (ASIM) provides an interim component that facilitates the integration of Multi-AEGIS Site Emulator (MASE) and other legacy sensors with the Air Command and Control System (ACCS) in scope of the ACCS First Level of Operational Capability (LOC1). ASIM enables this integration by translating Non-AWCIES (ACCS-wide common interface exchange standards) sensor data, i.e. plots, strobes and radar status messages into equivalent AWCIES messages and forwarding to ACCS for processing when applicable. Working the opposite direction as well, radar control actions from the ACCS operator is translated from AWCIES by ASIM into sensor-specific messages, when applicable. Additionally, ASIM automatically provides sensor status data required by ACCS to declare the sensor link operational.

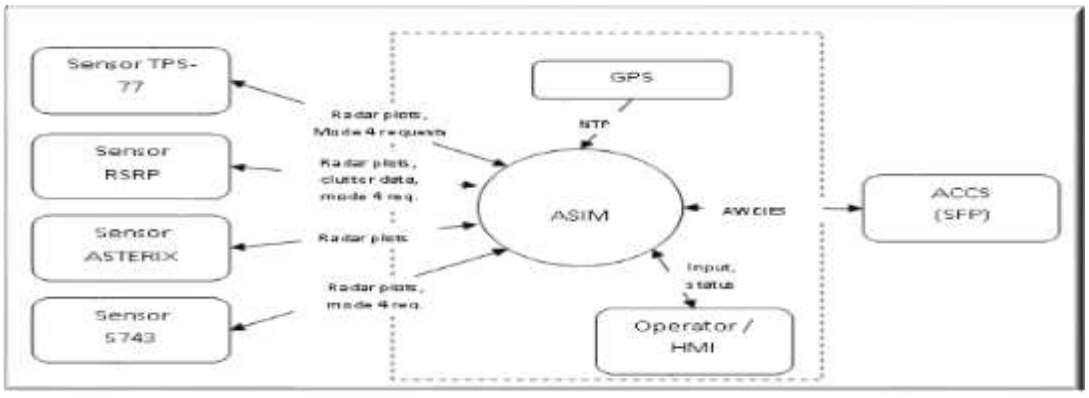
Value Proposition: ASIM Service provides a standard solution for interfacing non-AWCIES compliant sensors with the ACCS. The translation and exchange of data is fully automated and does not require operator attention. ASIM enables data to managed easily, where AWCIES data into and out of ACCS can be recorded/replayed and dumped in real-time for analysis by running ASIM provided programs on the ACCS servers. All data passing through ASIM is available for analysis.

Service Features:

Sensor Integration

- ASIM connects legacy sensors with ACCS and provides target reports.
- If a sensor can be controlled, e.g. Mode 4 interrogation, ASIM allows these orders to be translated and sent to the sensor.
- The exchange of data is fully automated and does not require operator attention.
- Failures are logged to a non-volatile media.
- Safety related events are also forwarded to ACCS by ASIM as radar failure reports.
- In principle, ASIM appears to both ACCS and sensor as a transparent system. However, if target reports have an inconsistency between time and azimuth (which can lead to reduced tracking performance of ACCS) ASIM is able to reduce this error based on reference data from the sensor.

The figure below outlines ASIM in a typical use case:



Supported configuration

- ASIM typically consists of two servers, one hosting the sensor interface and the second providing the data to ACCS or any other consumer. The two-server configuration supports to separate different security levels between the sensors and ACCS. A boundary protection system, typically based on an application layer firewall, can be optionally placed between the two ASIM servers.
- ASIM supports two configurations, a single and a split configuration:
  - *In a single configuration*, direct interfaces to sensor data and the ASIM servers are installed at a single location, usually at the ACCS location.
  - *The split configuration* supports geographical separation of the direct sensor interfaces from the ASIM server connected directly to ACCS. This also supports that multiple remote sensor interface servers can connect to one server which provides the data to ACCS.

Supported sensor/interface standards: JASR8, RMP, DDL, (A)S29, RAT31DL, HADR, CD2, RSRP, S743D, AWCIES, T101, Cardion, T92, SRT, ASTERIX

Other hardware, software and CIS details

- Uses NCI Agency (NPC) Integrated Solaris platform (NISP) as a secured Solaris OS platform
- X86 or SPARC based server HW able to run NISP/Solaris

Service Flavours: The Service is available in two flavours: the recent and the previous releases installed in the field.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret

Service Prerequisites:

APP050 ACCS Application Service

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training

- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF029 - NATO High Frequency (HF) Support Service

Service ID: INF029

Service Name: NATO High Frequency (HF) Support Service

Portfolio Group: Infrastructure Services

Service Status: Pipeline

Service Description: The High Frequency (HF) Support Services are mainly provided via NATO BRASS (Broadcast, Ship-Shore) system which is designed to support all NATO Maritime missions. The Service provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks and timely, accurate and reliable command and control communications and information exchange with NATO message switching and distribution capabilities.

There are NATO and nationally owned BRASS stations. National stations offer BRASS services to NATO based on Memoranda of Understanding signed with ACO. During the development, implementation and in-service support of NATO BRASS, NCI Agency has gained invaluable knowledge and is offering:

- Budgeting and financial mechanism to manage NATO funds granted for BRASS services delivered to NATO by Nations.
- In service support to BRASS Automated Control and Management Systems (ACMS).
- Support for BRASS Initial Core Capability (ICC) software.

Value Proposition: The HF Support Services offered for BRASS System provide:

1. Proficient budgeting and financial structure in place with know-how of NATO procedures.
2. Long experience gained during the in-service support of NATO BRASS sites.
3. Expertise on the BRASS ICC software supported by the capabilities of the BRASS System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) facility located in NCIA Mons.

Service Features: The main features of NATO HF Support Services are:

- Existing budgeting and financial mechanism to manage NATO funds granted to pay for BRASS services delivered to NATO by Nations. Currently, NCIA manages funds for HF services delivered by Portugal to NATO.
- In service support to BRASS Automated Control and Management Systems (ACMS). NCIA was managing the NATO ACMS nodes and HF stations before they were handed over to the Host Nations. NCIA supports the NATO ACMS in Northwood.
- Support for BRASS Initial Core Capability (ICC) software for the Nations that use it and may decide to use it in the future. The software baseline and source code and documentation is available for free to NATO nations. BRASS ICC software support and maintenance activities are performed in the NCIA BRASS System Test Integration Verification Reference Maintenance and Diagnostic Facility (STIV RMD).

Service Flavours: This Service is available as a single flavour.

Available on: NATO Unclassified

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF032 - DCIS - Small Deployable Military Bandwidth SATCOM Terminal (DMBST) – BBSST & DART Terminals Service

Service ID: INF032

Service Name: Small Deployable Military Bandwidth SATCOM Terminal (DMBST) Service

Portfolio Group: Infrastructure Services

Service Description: The Small DBMST Service consists of the Dual-band Auto-pointing Rapid-deployable Terminal (DART) and Bi-Band Satellite Suitcase Terminal (BBSST) SATCOM Terminals which are a Deployable CIS that provides Communication and Information Systems to deployed commands of the NATO High-readiness Response Force (NRF). The requirements of the rapid reaction forces require a capability to support up to 126 staff and enable them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission-partnering Nations and non-governmental organisations.

These SATCOM terminals have been reassigned from ISAF for use in fulfilling AOM and Exercise requirements.

Value Proposition: The Service extends C2 Services worldwide, thus enabling Operational Commanders to execute NATO Council Approved Operations worldwide. The DART terminals provide a small X and Ku band rapidly deployable SATCOM capability. The BBSSTs are also X and Ku band capable; and BBSST equipment is contained within a suitcase for improved transportability.

Service Features: The features of the Small Deployable Military Bandwidth SATCOM Terminal Service are:

CIS Assets:

- DUAL BAND AUTO POINTING RAPIDLY DEPLOYABLE TERMINAL (DART)
- BI-BAND SATELLITE SUITCASE TERMINAL (BBSST)
- IP Telephones
- HP Server Hardware
- Laptops
- Printers/ MFDs

The DART Terminals provide the following services:

- Rapidly deployable capability,
- X-Band SATCOM Bandwidth,
- Ku Band SATCOM Bandwidth.

The BBSST provide the following services:

- Rapidly deployable capability,
- X-Band SATCOM Bandwidth,
- Ku Band SATCOM Bandwidth.

Non-CIS Assets: Uninterruptible Power Supply (UPS), Tent, CVRT (type SHERPA), Trailer, PGS.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours:

1. DART SATCOM Terminal
2. BBSST SATCOM Terminal

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Qualified Operators

Standard Service Support Levels:

Service Availability[1] **Target:** 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: In accordance with terms agreed in SLA

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF033 - DCIS - TACSAT (UHF) Service

Service ID: INF033

Service Name: TACSAT (UHF) – Deployable Communications & Information Systems (DCIS) Service

Portfolio Group: Infrastructure Services

Service Description: The DCIS Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Service provides CSC Service Description Code: SCS8 - Radio Communications Services. Each of the UHF TACSAT Systems is capable of providing secure voice and data. All radios provide the NRF components with a tactical robust deployable communications system. The UHF TACSAT Radios consist of an AN/PRC 117F UHF radio with either a static directional antenna or an omnidirectional vehicle-mounted antenna.

Value Proposition: NATO's UHF network is a set of complex systems which enables NATO forces access to a secure tactical radio SATCOM network across all of NATO's Areas of Responsibilities (AOR's). The UHF SATCOM capability is used to support NATO Land, Sea and Air operations (on-the-move, on-the pause and static) using both Demand Assigned Multiple Access (DAMA) and Single Channel Per Carrier (SCPC) channels, as required, to provide secure voice and data capabilities. NATO UHF terminals are used in support of ACO requirements.

Service Features:

The UHF TACSAT radios can be configured as the On-The-Pause (OTP) or the On-the-Move (OTM). This service consists of:

- UHF TACSAT Terminal
- Radio Ancillary Equipment
- Antenna System
- Ni-MH Rechargeable Batteries

Service Prerequisites:

Reliant upon - INF012 SATCOM Service

Service Flavours: Different flavours of the MPC Service the customers can choose from are:

1. Static (On-The-Pause)
2. Mobile (On-The-Move)

Available on: N/A

Standard Service Support Levels:

	Availability[1] Target	Service Restoration Period
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

PLATFORM SERVICES

V3.4

This page is left blank intentionally

PLT001 - Web Information Publishing and Portal Service

Service ID: PLT001

Service Name: Web Information Publishing and Portal Services

Portfolio Group: Platform Services

Service Description: The Web Information Publishing and Portal Services provide an auditable, secure, online collaborative environment for users to create, capture, store, manage, broadcast, publish, view and search all types of digital content. Users of the service are able to publish content directly, without the intervention of a web master. This service enables organizational elements to establish an intranet or extranet rich collaboration environment by utilising and combining web information publishing and portal services feature options. This will enable collaboration and social capabilities in the context of team, community, NATO enterprise and Alliance/External entities (federation).

Value Proposition: The Web Information Publishing and Portal Services allow users to work together much more effectively, sharing information, jointly working on documentation etc. without the requirement to send it to a group of individuals and then compile responses. The offered collaboration and social services are an enabler for an effective knowledge management. This auditable, joint approach significantly decreases the time required and improves information flow and understanding across all users.

Service Features: The Web Information Publishing and Portal Service provides the following features (subject to the available network):

- Web Publication
  - Top Home Page
  - Page
  - Web Publishing Workflow
- Collaboration
  - Collaboration template supporting among others
    - Team Collaboration Site
      - Document libraries, Lists, Task Lists, Project Sites, and Sites.
    - Community site (Community Portal).
  - Events Calendar
  - Wiki
  - Notifications
  - Surveys
  - Web app One Note
- Broadcast (presentation, audio, video)
- "MySite" (including personal online storage space)
  - Newsfeed (Create and view posts and updates in your Newsfeed).
  - Microblogging features.
- Search capabilities.
- Management, Maintenance, Development, Integration
  - Maintain user profiles.
  - Optional Web content authoring.
  - Optional Site customization.
  - Optional Workflows support.

- External data access (BI connectors).
- Security management and site management.
- Optional Integration with business applications.

Service Flavours:

NATO Information Portal (NIP): SharePoint NATO SECRET Site Collection with 10 GB (expandable) of storage.
NATO Standard collaboration platform: Sharepoint Site Collection with 10GB (expandable) of storage.
NATO NU extranet web publishing and portal (up to and including NATO Unclassified)
Optionally, additional storage is available for each flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

WPS002 - User Access Service
WPS003 - Enterprise User License Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT002 - Combined Federated Battle Laboratory Network (CFBLNet) Service

Service ID: PLT002

Service Name: Combined Federated Battle Laboratory Network (CFBLNet) Service

Portfolio Group: Platform Service

Service Description: The Combined Federated Battle Laboratories Network is a multinational, research, development, training, trials and assessment infrastructure for C4ISR, based on a multinational IP backbone with managed enclaves on top in support of the initiatives. Infrastructure reuse for multiple multinational and concurrent initiatives is a key element for the CFBLNet mission partners. CFBLNet operates as a true federation; no single nation owns the CFBLNet, where each member is responsible for provisioning and operation of its own sites and systems. CFBLNet fulfils the need for persistent joint multinational and cost effective infrastructure. The capability allows for various partnerships; CCEB, NATO, bilateral and multilateral. CFBLNet was established in 2001 and is continuously improving its services to provide the best and most cost effective federated infrastructure in support of its mission. Currently its scope consists of 35 mission partners: all 28 NATO Nations and Austria, Australia, Finland, New Zealand, Sweden, Switzerland and the NATO organization. CFBLNet is open through sponsorship to additional partner nations. As a prerequisite, customers are asked for valid security accreditation and related MSAB Site and Initiative National/NATO accreditation endorsement certificates (S-, I- NAEC's).

Value Proposition: CFBLNet provides the Multinational federated coalition network infrastructure of choice to facilitate all potential non-operational activities to support the war fighter. The single CFBLNet network infrastructure with many partners and initiatives, saves cost, increasing their quality, lower their risk and reduce setup time. CFBLNet offers an agile and fully service based non-operational network infrastructure, and operates at up to a Secret releasable accreditation level. CFBLNet provides common framework, well defined processes, security procedures and agreed technical standards.

Service Features: The Combined Federated Battle Laboratory Network (CFBLNet) Service offers the following features:

- Access points (connection to Core up to 50Mbps)
- Network Services (Routing, encryption, switching, DNS, NTP, network management, testing)
- Service Desk (3hrs/month)
- Coordination with Nations
- Representation for sponsored nations
- Coordination for NATO
- Initiative / CIIP support
- Limited email (<20 accounts)
- Chat in standing enclaves (Chat server)
- Web Services for initiatives (Microsoft Web server)
- VOIP (Cisco Voice server)
- VTC in standing enclaves (VTC MCU in RED, Pink and CUE enclaves (Acano/Cisco))
- SharePoint in standing enclaves (Sharepoint server)
- Data Diodes (Low-> High file transfer)

- Anti-virus / WSUS (Antivirus and Windows update servers for automatic updates (AFPL approved and regular versions)
- Simulation of CFBLNet (optional) (simulation of nation/organisational node for testing)
- Flow audit in standing enclaves
- Additional access bandwidth (optional)

Service Flavours:

1. National CFBLNet access to the European CFBLNet Core infrastructure and services in support for RDT&A, Testing, Training and Exercises.
2. NATO organisation access to the NATO CFBLNet PoP core infrastructure and services in support for RDT&A, Testing, Training and Exercises.

A. During initiatives
B. Outside initiatives

Features	Flavour 1	Flavour 2
	National	NATO Organisations
Core Access Points	●	
NATO Access points		●
Network Services	●	●
Service Desk	●	●
Coordination with Nations	●	●
Representation for sponsored nations	●	
Coordination for NATO		●
Initiative / CIIP support	●	●
Limited email	●	●
Chat in standing enclaves	●	●
Initiative Web Services	●	●
VOIP	●	●
VTC in standing enclaves	●	●
SharePoint in standing enclaves	●	●
Data Diodes	●	●
Anti-virus / WSUS	●	●
Simulation of CFBLNet (opt)	●	●
Flow audit in standing enclaves	●	●
Full local access node provisioning and operation		●
Additional access bandwidth	Optional	●

Available on:

CFBLNet NS
NS (REL)
NR (REL)
NU
NU (REL) for various NATO and Coalition communities

Service Prerequisites:

National subscribers: Link between National CFBLNet PoP Infrastructure and European and NATO CFBLNet NOC Core infrastructure. Options: NGCS/LTX, national leased line, alternative linkage.

NATO Organisational subscribers: Link between NATO Organisational CFBLNet Access Node and NATO CFBLNet PoP infrastructure through NGCS/LTX. (Alternative if NCGS is not possible: leased line, satcom, alternative linkage).

The European and NATO CFBLNet NOC/PoP has link termination points at Telecity II Amsterdam (commercial), NATO HQ (NGCS/LTX), NCIA Mons (NGCS/LTX) and NCIA The Hague (NGCS/LTX and commercial).

Standard Service Support Levels:

Service Availability[1] Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT003 - Web Hosting Service

Service ID: PLT003

Service Name: Web Hosting Service

Portfolio Group: Platform Services

Service Description: Web Hosting Services, provides a fully managed, (shared or dedicated) scalable platform on which a user can host web applications and/or web sites. Additionally, this service provides users with the capability to host a basic MS SharePoint collaboration platform and/or portal in an internet/extranet environment. The service can be provided in a high-availability modus for customers seeking a higher level of performance, availability and reliability. General features of the service include; caching, performance monitoring, platform maintenance, scalability, and security.

Value Proposition: Web Hosting Service offers the user multiple benefits; comprising of:

- Scalability; ensuring resource is available as and when the Web Hosted Application Service needs it, ensuring no delays in the in expanding capacity or the wastage of unused capacity.
- Lower Total Cost of Ownership (TCO) of a Web Hosted Application Service provided through a shared and managed Infrastructure model.
- Location Independence; Web Hosted Application Service can be accessed from any location with Internet Connectivity, subject to security protocols that would allow this.
- Physical Security; physical security afforded to the servers which are hosted within a secure environment.
- No Single Point of Failure; if one service fails the broader service can remain unaffected, ensuring service availability and reliability.

Service Features: The Web Hosting Service offers the user the following features:

- PaaS: Fully managed Platform. A fully managed hosting environment provides a maintained and operated platform, thus ensuring users can focus on the implementation and operation of the application
- Operational Support (including but not limited to Performance Monitoring, Technical Support).
- Optional Load balancing Service Usage of Web Application Services ensuring availability.
- Secure Web Application Services through Access Management (through the available standard options in IIS, Apache, SharePoint).
- Support for standard web protocols, included but not limited to: HTTP, HTTPS (SSL), FTP.
- Three tier architecture (SOA), separating presentation layer, application layer and database.
- Server side frameworks and languages supported, among others:
    - Java
    - ASP.NET
    - PHP
    - Ruby
- NATO required Security features and tools.
- Web/application servers available: Apache, Microsoft Internet Information Services (IIS).
- Provisioning of SharePoint platform to support hosting of SharePoint based portals.
- Provisioning of Basic SharePoint Collaboration Platform for Intranet/Extranet

Service Flavours: The flavours listed below for the Service are available on the supported web hosting platforms (Microsoft Internet Information Services (IIS), Apache and SharePoint).

- Shared High-availability web hosting platform (load balancing with multiple web-servers)
- Dedicated Standard web hosting platform
- Dedicated High-availability web hosting platform (load balancing with multiple web-servers)

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Public Internet Access (PIA) Gateway, security classification up to and including NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	98.0 %	4 hours

Note: Availability of the "web hosting service" is primarily dictated by the availability of the underlying infrastructure services, i.e. "Infrastructure Hosting Service".

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT006 - Database Platform Service

Service ID: PLT006

Service Name: Database Platform Service

Portfolio Group: Platform Services

Service Description: Database Platform Service provides a fully managed, scalable database platform for use as an integral part of a production, testing and/or development environment. Service provides flexible, scalable, and demand based platform, which is oriented toward central monitoring and management where underlying complexities of Database technologies (Oracle, MS SQL, MySQL, PostgreSQL…) are encapsulated as a generic service.

Value Proposition: Database Platform Service offers the user the following benefits:

- Lowered Total Cost of Ownership of a database through the provision of a consolidated, standardized and volume managed database environment.
- Agility to meet NATO demands through provision of standardized, tested environments.
- Size and growth of a database is monitored and provision of required capacity made to ensure continued availability and performance to meet operational needs.
- For standard use the underlying technical complexities are isolated from the customers.
- Increased security and availability since dedicated team of experts will monitor these services.

Service Features: Database Platform Service offers the user the following features:

- Database hardware capacity to run the service.
- Lifecycle management of the Database Platform.
- Database software licensing and maintenance.
- Centrally managed and automated backup with point-in-time recovery, and patching and upgrades.
- Full database and transaction log backups for Point-In-Time database recovery.
- Fully managed database server; data Files, Transaction Logs and Database backups.
- Operating System and Database Administration. (Software Installation and Maintenance, System-level patching and support)
- System and database monitoring.
- Fully managed operating platform infrastructure
- Full platform administration services.
- Capacity provisioning through scalable and flexible management of available resources

Service Flavours:

- Oracle shared high-availability database platform service.
- Oracle dedicated Single Instance database platform service
- Oracle dedicated high-availability database platform service
- SQL Server shared high-availability database platform service
- SQL Server dedicated Single Instance database platform service
- SQL Server dedicated high-availability database platform service

Available on:

NATO UNCLASSIFIED
NATO RESTRICTED

Public Internet Access (PIA) Gateway

Service Prerequisites:

None

Standard Service Support Levels:

Service Flavour			Availability[1] Target	Restoration Period
Level 1	High Availability (Failover Clustered Instances Or Database Mirroring)	During Support hours	99.9 %	1 hour
		Outside Support hours	98.0 %	4 hours
Level 2	Single Instance Database	During Support hours	99.0 %	4 hours
		Outside Support hours	98.0 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT007 - DCIS - Afloat Command Platform (ACP) Service

Service ID: PLT007

Service Name: Afloat Command Platform (ACP) Service

Portfolio Group: Platform Services

Service Description: The Afloat Command Platform (ACP) is a Deployable CIS that provides limited Command and Control (C2) Communication and Information Systems to deployed commands of the NATO high readiness Response Force (NRF). The ACP was initially procured to support the NRF Deployable Joint Staff Element (DJSE) and designed to exercise command and control from on-board a maritime asset. The current ACP PoPs are operational but they do not provide any Functional Services capability. The ACP is the same technological standard as the LINC-E capability.

Value proposition: The ACP consists of CIS equipment providing secure and non-secure voice, data, and video for up to 100 Deployed HQ staff integrated into the existing CIS architecture of vessels which are nominated as the ACP (without transmission element). The ACP system can provide the operational user community of 100 with the core of NCI Agency provided CIS services.

Service Features: The ACP provides the following NCI Agency-provided CIS services in a deployable format:

- Voice communication services,
- Video teleconferencing (VTC),
- Email,
- Internet/Intranet Web browsing,
- Data transfer,
- Data / file storage,
- Hardware, and
- Printing / scanning / plotting Services.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites: N/A

Standard Service Support Levels:

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

PLT008 - DevOps Service

Service ID: PLT008

Service Name: DevOps Service

Portfolio Group: Platform Services

Service Status: Pipeline

Service Description: The DevOps service is an enabling service consumed by NCI Agency Service Lines – Functional Area Services teams to manage C4ISR Capabilities' lifecycle via the provided platform and engineering toolchain. It is composed of environments and tools that enables the NCI Agency SW Factory, which is the collaboration space where NCI Agency collaborate with Industry and Nations. It is Platform as a Service (PaaS) type of service and it sustains the following processes:

- Requirements Management
- Architecture & Design
- Development
- Continuous Integration (Build)
- Test Automation
- Continuous Delivery (Deploy & Release)

Value Proposition: The Service is a fundamental enabler of NCI Agency SW Factory PFE (Purchaser Furnished Equipment) where:

1. The Agency exploits its own Software Factory in which development is performed under common (Agency / community) standards using common tooling;
2. It represents mandated PFE in procurements;
3. Through self-service cloud provisioning, suppliers working on projects or service adaptation can deploy standard environments for development, testing and regression testing;
4. These environments can be populated with test instances of all services that the component under development consumes;

The benefits of the Service include:

- Enabled end-to-end traceability from the original operational requirements to the implemented solution components;
- Establish the intended collaboration (technology and practices) with Industry;
- Increased quality of FAS releases through traceability, real-time progress information, ongoing/recurring testing and through feedback loop for production incidents;
- Increased manageability through centralization and automation**;**
- Enable iterative and faster SW releases (release cadence);
- Better instruments to manage portfolio;
- Better control over IPR;
- Easier on boarding of new staff due to alignment with industry methodologies and best practices;
- Improve the efficient use of valuable resources (Staff, Infrastructure, Funds);
- Enable planned and implemented reuse of SW components;
- Reduced cost of development and application deployment (installations).

Service Features: The DevOps Service offers hybrid cloud development environments to Functional Area Services (FAS) teams to improve the cost predictability and administration of new developments.

It also offers the service platform used by FAS team as development and testing environments, and it includes the needed **toolchain** that is based on both Microsoft, and Open Source ecosystems to ensure coherency with NATO C4ISR Technology architectures.

PROCESS	TOOLCHIAN
REQUIREMENTS	IBM Doors NG
ARCHITECTURE	ARIS
	Archi
DESIGN	Enterprise Architect
CODE	Microsoft Visual Studio Team System
	GitLab
WORK ITEM	Microsoft Visual Studio Team System
	Atlassian JIRA
BUILD	Microsoft Visual Studio Team System
	Jenkins
DEPLOY	Microsoft Visual Studio Team System
	Nexus, Docker & EDML
TEST	Microsoft Visual Studio Team System
	Testrail
RELEASE	Microsoft Visual Studio Team System
	Nexus

Service Flavours: The flavours for the Service are available based on combination of the Service features, as follows:

- Requirements Management
- Architecture
- Development & Test
- Collaboration
- EDML (media delivery)

Available on:

Hybrid and Public Cloud (NU)

Service Prerequisites:

Procured licences for software used for provision of the service, in accordance with selected service flavours (toolchain).

Standard Service support levels*:* N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

This page is left blank intentionally

SUBJECT MATTER EXPERTISE (SME) SERVICES

V3.4

This page is left blank intentionally

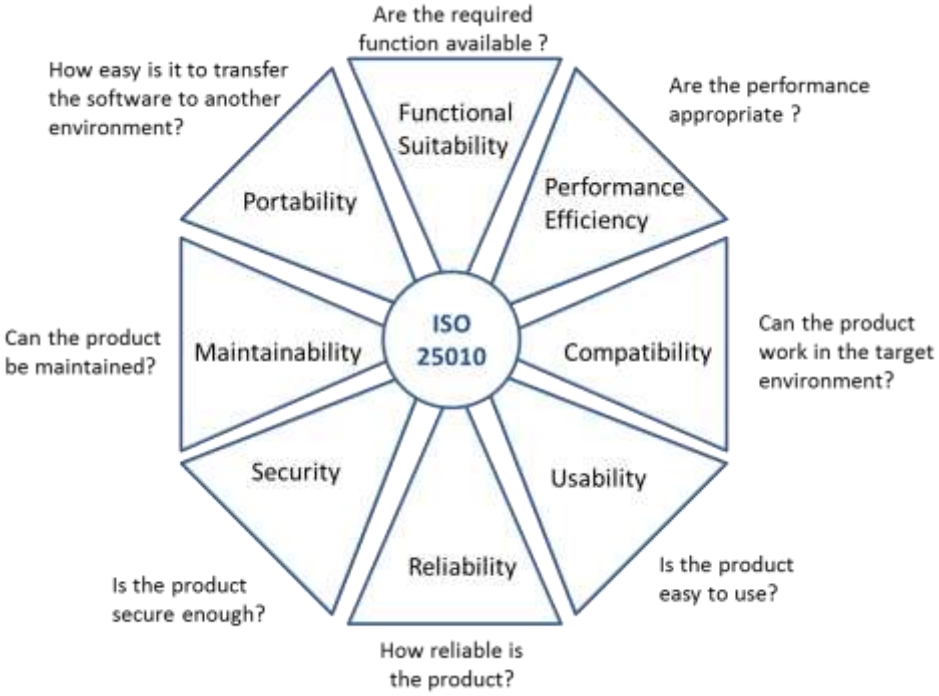
SME001 - IV&V Subject Matter Expertise Service

Service ID: SME001

Service Name: IV&V Subject Matter Expertise Service

Portfolio Group: Subject Matter Expertise

Service Description: The main objective of this service is to coordinate and plan all Test, Verification and Validation (TVV) activities covering the full lifecycle in support of the Project Manager, Programme manager or exercise director. The goal of TV&V is to ensure the quality of services, systems and products prior to deployment in the live environment. TV&V activities therefore focus on the key quality characteristics:



Value Proposition: The purpose of Verification & Validation is to ensure the quality of products, services and systems. Independent V&V provides an impartial assessment of whether or not the output of a given activity satisfies the requirements of that activity and meets the needs of the user. V&V is undertaken at every stage of the lifecycle in order to identify and correct defects as early as possible in the project lifecycle in order to minimise impact on cost and schedule.

Service Features: The IV&V Subject Matter Expertise Service offers the user:

1. Support Type B Cost Estimate (TBCE) and IFB Development
2. Support Requirements Development and Review to ensure their testability
3. Provide Independent Witness to Factory/System/User Acceptance phase
4. Independent V&V of Non-Functional Requirements
5. Optional support to the PM or programme with SME, technical resources or policy/process/procedural assistance:
    - Provide assistance to project/engineering testing.
    - Provide assistance with test management tools.
    - Provide support to integration testing.

- De-risking test.

Service Prerequisites:

None

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Standard Service Support Levels: N/A

SME002 - IV&V Testing for Change Management Service

Service ID: SME002

Service Name: IV&V Testing for Change Management

Portfolio Group: Subject Matter Expertise

Service Description: This service covers the impartial change evaluation conducted by IV&V Service Line as part of the overall change management process. This service consists of testing performed on the Agency Reference Environment (including Coalition Interoperability Assurance and Validation (CIAV) testbed) requested by Change Managers. The trigger for this process is a Request for Change (RFC) submitted to the Change manager. IV&V Service Line proposes a test approach based on the quality criteria listed in ISO/IEC/IEEE 29119-4. This evaluation provides the requestor with the necessary objective evidence of the suitability of the system or service prior to deployment into the live environment.

Value Proposition: IV&V tests for Change Management are performed in order to provide objective evidence that the product, system or service under test is of satisfactory quality and meets customer, technical and security requirements. The tests will allow to identify defects and enable them to be corrected as early as possible in order to limit the risk of end-users finding failures when the system will be deployed in the live NATO environment.

Service Features:

- Review of supporting materials (RFC Release Package)
- Writing of the Test procedures and test cases
- Test Readiness Review (TRR) meeting
- Reference Environment Configuration and setup
- Test execution
- Test report

Service Flavours:

Patch testing: compatibility and reliability tests of software patches, i.e. software that provides corrective fixes for security vulnerabilities and other defects in Commercial Off The Shelf, NATO Off The Shelf or Open Source software. Patch tests are conducted by the IV&V SL, supported by other SLs, under the direction of the Patch Change Advisory Board (CAB). Patch tests include testing of Microsoft security updates under the Microsoft Security Update Verification Program.

COTS testing: product evaluation (the initial step of testing involves COTS). Where all the components – the COTS and the non-COTS components, are tested individually to assure their proper functioning. The tests assess whether the systems in the COTS Based System are compatible to each other and are yielding acceptable results or not. How far the results obtained are reliable is also tested as is the level of reliability of the system as a whole which implies the functional and nonfunctional testing have to be done for all required end to end business processes. Another key factor is maintainability. COTS tests are conducted by the IV&V SL, supported by other SLs

FAS testing: Functional testing of the service including user Interface (UI), automated functional testing with good test data and test tool. FAS tests are conducted by the IV&V SL, supported by other SLs

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret (NATO Secret Releasable to xx)

Service Prerequisites:

SME001 – IV&V Subject Matter Expertise

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SME003 - Interoperability Assurance Subject Matter Expertise Service

Service ID: SME003

Service Name: Interoperability Assurance SME Service

Portfolio Group: Subject Matter Expertise

Service Description: This service offers Interoperability Assurance Subject Matter Expertise for systems and services during bi-lateral, multilateral or coalition test events (demonstration, formal testing on reference testbeds or exercises). This service consists of testing or witnessing performed on local and/or distributed exercise or reference environments. It provides the customer with objective evidences of the interoperability function and suitability of the system or service as deployed in the testing or exercise architecture.

Value Proposition: Interoperability Assurance SME Service are available to perform verification and validation showing that the product(s), system(s) or service(s) under test is of satisfactory quality and meets customer, technical and/or security requirements. The tests will allow to identify defects and enable them to be corrected as early as possible in order to limit the risk of end-users finding failures when the system will be deployed in the live bi-lateral, multilateral or coalition environment.

Service Features: The Interoperability Assurance SME Service offers the user:

- Review of supporting materials
- Writing (support) of the Test procedures and test cases
- Test Readiness Review (TRR) meeting
- Interoperability Assurance Reference Environment Configuration and setup
    - Local, distributed or deployed.
- Test witnessing
- Test execution
- Test report
- Test result assessment

Service Flavours: The flavours of the Interoperability Assurance SME Service, the customers can choose from are:

1- Interoperability Assurance testing between NATO systems and services and National and/or other international systems and services. (e.g. Coalition Interoperability and Assurance Validation (CIAV).
2- Interoperability Assurance testing between NATO systems and services during exercises.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret (NATO Secret Releasable to xx)

Service Prerequisites:

SME001 IVV Subject Matter Expertise Service

Standard Service Support Levels: N/A

Service Cost / Price: The Service cost depends on the number of systems and services it requires to test against, their complexity, the test scope, the test location (local and/or distributed), and the number of test runs. Therefore, it is calculated specifically for each service delivery.

SME004 - Provision of Subject Matter Expertise on Federated Mission Networking (FMN) Service

Service ID: SME004

Service Name: Provision of Subject Matter Expertise on Federated Mission Networking (FMN) Service

Portfolio Group: Subject Matter Expertise Services

Service Description: This service provides:

- Subject Matter Experts (SME) to the governance, management and working group structures that support the direction and development of the FMN Framework.
- Monitoring and reporting of the progress to apply approved federation solutions in common-funded capabilities.
- Derisking of the implementation of FMN Spiral Specifications prior to use in support of NATO-led Missions through collective and federated CIAV testing with other Affiliate Nations
- A service management authority (SMA) to oversee the design and operation of federations of NATO and National Mission Networks in support of NATO-led Missions (e.g. eNRF).
- Operational analysts and technical SME to evaluate/confirm the compliance of federations of NATO and National Mission Networks to the FMN Framework.
- SME for the provision of FMN training.
- SME to support briefings on FMN and to support communications and awareness campaigns.
- SME to provide advice on the federation of National Networks with NATO networks and on federations within coalition and national federations.

Value Proposition: With NAC approval of NFIP Vol 1, NATO committed the NATO Command Structure (NCS) to be an FMN Affiliate alongside the Nations with the level of ambition to provide a Mission Network Extension (MNE) for NATO-led Missions. To meet the requirement associated with such ambition, the ability to provide certain capabilities is necessary. Without committing resources and expertise, NATO will be unable to fulfil its role as the key contributor to and facilitator of the FMN framework, which will undermine the whole purpose of FMN and NATO's lead role in it. Additionally, NATO has also committed itself to apply FMN to all eNRF operations and has stated that this is the interoperability, to which the NFS is to adhere to. SACEUR has also offered eNRF exercises as venues for the National FMN Affiliates, to routinely confirm adherence to the FMN framework. As a member of CIAV, the NCS FMN Affiliate is also responsible to the other Affiliates to collectively de-risk upcoming federated capabilities.

Service Features: The Service provides the following areas of expertise and facilities:

- Support to FMN Governance and Management:
  - Support to the FMN Governance structures. Provision of support to the MCWG (CIS) on the governance of the FMN Framework. Provision of support in assessing the impact of federation on C3 Policies and Directives. Provision of support to the rolling maintenance of the FMN standards profile within the NISP. Provision of support to the C3B and its substructures on federation topics;
  - Support the FMN Management Group. Provision of support to the NCS FMN Affiliate POC in the FMN Management Group (ACOS J6);

- Support the FMN Secretariat. Provision of Change Implementation Coordinator (CIC) within the FMN Secretariat, provision of FMN Secretariat with DNBL FMN Portal infrastructure;
- Support the FMN Operational Coordination Working Group. Provision of Operational Analysis Expertise to OCWG;
- Support the FMN Capability Planning Working Group. Provision of support to development of the FMN Spiral Vision and Roadmap. Provision of segment architectural expertise to the development of technical service instructions. Provision of operational analysts and functional experts to the development of procedural instructions. Provision of operational analysis support to maintain alignment between FMN and the NATO Defence Planning Process (NDPP);
- Support the FMN Multinational CIS Security Management Authority. Provision of Cyber Security expertise to the MCSMA;
- Support the FMN Coalition Interoperability, Assurance and Validation (CIAV) Working Group. Provision of IV&V expertise to the CIAV WG. Provision of standardised test requirements and test cases for interoperability events;
- Support the FMN Change and Implementation Coordination Working Group. Provision of Service Management and Service Engineering expertise to the CICWG. Provision of Change Management support for the FMN Baseline. Provision of Service Engineering to derive templates for Joining, Membership and Exit Instructions. Provision of Architecture Software and Reach for Remote National Service Engineers;

- Programmatic monitoring of the implementation approved federation solutions in common-funded capabilities:
  - Support decision making within the NCS FMN Affiliate. Provision and maintenance of rolling Gap analyses. Preparation of information and decision briefs for the C3CG. Provision of progress reports on the implementation of approved federation solutions in common-funded capabilities (especially NATO DCIS);
  - Support resourcing and internal coordination. Provision of FMN Coordination/programme office;
- Support to de-risking of the implementation of FMN Spiral Specifications prior to use in support of NATO-led Missions:
  - NCS FMN Affiliate CIAV Test Director;
  - Test Team in Support of NCS FMN Affiliate Assessments;
  - NCI Agency FAS SME to Support FMN Matters ;
  - NATO CV2E Lab Facilities;
  - CFBLnet Connectivity for NATO FMN CIAV lab;
  - Support Assurance, Validation and Verification (AV&V) of NATO systems at CWIX to ensure their compliance with up-coming FMN Spiral Specifications;
- SMA to oversee the design and operation of federations of NATO and National Mission Networks in support of NATO-led Missions and exercises:
  - SMA Design Authorities (DA) / Technical Authorities for each federated service in preparation for and at planning conferences;
  - Joining Membership and Exit Instructions for the federation of NATO and National Mission Networks;
  - SMA Operating Authority Change Manager (ChM) in preparation for and at planning conferences;
  - Cyber Security support to the MN Security Accreditation Board (SAB);
  - SMA Operating Authority (OA) presence in the DNOC in the execution phase;

- SMA OA ChM (and CAB) for duration of MN;
- NRF SAB lead for the maintenance of the Community Security Requirements Statement (CSRS) for duration of MN;

- Support to the evaluation/confirmation of the compliance of federations of NATO and National Mission Networks to the FMN Framework:
  - Service Engineers to a Technical Assessment team;
  - Service Management experts to a Mission Network instantiation Procedural and Organisational Assessment team;
  - Operational analysts and functional experts to a Mission Thread assessment Team;
- Support to FMN Training:
  - Material for general and specialist FMN training courses;
  - SME to brief on FMN topics within training courses;
  - SME to support FMN Training Requirements Analyses. Provide SME to support FMN Training Needs Analysis;
- Support to briefings and FMN communications and awareness campaigns:
  - Support the development of an FMN Communication and Awareness Plan;
  - Material for general and specialist consumption;
  - SME to brief on FMN topics;
- Advice on the federation of National Networks with NATO networks and on federations within coalition and national federations:
  - Technical consultancy on options to connect networks.

Service Request: Dependent on the customer funding lines, services may be requested as follows:

- ACO funded (routine): via the CSLA;
- ACO funded (temporary or new): via CRF and a resulting ACO POW project;
- ACT funded: via ACT POW;
- IMS funded: via NHQ C3S projects;
- Nationally funded: via CRF and a resulting Nationally funded project.

Service Flavours: The Service is available in multiple flavours, depending on the combination of features required.

Available on: The SME can provide services/advice through the following networks:

- Support to FMN Governance and Management: Unclassified/NR/NS
- Programmatic monitoring of the implementation approved federation solutions in common-funded capabilities: Unclassified /NR/NS.
- Support to de-risking of the implementation of FMN Spiral Specifications prior to use in support of NATO-led Missions: Unclassified /NR/NS/CV2E.
- SMA to oversee the design and operation of federations of NATO and National Mission Networks in support of NATO-led Missions and exercises: NR/NS/NSrelNRFxx.
- Support to the evaluation/confirmation of the compliance of federations of NATO and National Mission Networks to the FMN Framework: NS/NSrelNRFxx.
- Support to FMN Training: Unclassified /NR/NS
- Support to briefings and FMN communications and awareness campaigns: Unclassified /NR/NS
- Advice on the federation of National Networks with NATO networks and on federations within coalition and national federations: Unclassified /NR/NS

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SME005 - Acquisition Service

Service ID: SME005

Service Name: Acquisition Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Acquisition Service encompasses all activities in relation to procurement, including initiation, solicitation (request for quotations), negotiations, evaluation, contract management (including invoice payment), contract closure, and reporting. If required, the Service may include also Integrated Logistic Support and Cost Estimate & Analysis.

Value Proposition: The Service supports procurement activities of outsourced requirements in support of SLA implementation development.

Service Features:

Procurement: initiation, solicitation (request for quotations), negotiations, evaluation, contract management (including invoice payment), contract closure, and reporting;

Integrated Logistic Support: ensuring that all elements of logistics support of acquired systems/facilities are planned, engineered, acquired, tested and provided in a timely and cost-effective manner;

Cost Estimate & Analysis: provision of lifecycle cost estimates, price analyses and support to price negotiations.

Service Flavours:

Procurement:

AQ.CO.11: Simplified Purchasing/Sole Source encompasses procurement activities up to 20 k€;
AQ.CO.12: Simplified Purchasing/3 Tender – encompasses procurement activities from 20 k€ up to 40 k€;
AQ.CO.13: Simplified Purchasing/5 Tender – encompasses procurement activities from 40 k€ up to 160 k€;
AQ.CO.20: Simple Competitive Purchasing – encompasses procurement activities above Level D (160 k€), i.e full ICB process (Lowest Price Technically Compliant) as well as BOA procurement above that level;
AQ.CO.30: Complex Sole Source Contracting - encompasses procurement activities addressing complex sole source acquisition;
AQ.CO.40: Complex Competitive Contracting – encompasses procurement activities above Level D (160 k€), i.e full ICB process (Lowest Price Technically Compliant or Best Value) above that level;

Integrated Logistic Support

Cost Estimate & Analysis

Available on: N/A

Service Prerequisites:

Clear set of requirements provided in a timely manner to ACQ Directorate

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SME006 - Operational Analysis Service

Service ID: SME006

Service Name: Operational Analysis Service

Portfolio Group: Subject Matter Expertise Service

Service Description: Operational Analysis (OA) is a consultancy service, which consists of developing and applying fit-for-purpose approaches and scientific methods to analyse problems across the spectrum of defence activities, and supporting decision makers in understanding, visualising and resolving them.

Value proposition: The OA service offers reliable and timely expert support to decision makers in NATO and Nations. Professional analysts, who have an excellent understanding and extensive experience in defence and security issues, and supported by a comprehensive set of analytical supporting tools, are able to help scoping an issue that decision makers face and to provide objective analysis of available options, leading to better informed decision making. The OA experts have decades of involvement in defence planning support, OA support to Alliance Operations and Missions, and support to peacetime organisational effectiveness. They also have a proven track record of delivering high quality expertise and products to customers' satisfaction, on time and within budget. The extensive knowledge of OA experts on NATO's operational processes and their experience in providing operational analysis can quickly benefit decision makers at all levels.

Service Features: NCI Agency can provide ad hoc and flexible Operational Analysis consultancy to NATO and Nations through the application of tailored analytical methods to solve complex problems as typically faced by organisational leaders and operational commanders. The Service can provide support in a range of fields such as the following (non-exhaustive list):

Defence Planning: provision of a full spectrum of technical consultancy, analysis and advice to support NATO and the Nations in Defence Planning (DP), primarily with focus on support to the NATO Defence Planning Process (NDPP). It includes (non-exhaustive list):

- Analytic expertise in support of the NATO Defence Planning Process (NDPP) activities, including identification of capability requirements, apportionment of requirements, and suitability and risk assessment; this analytic support involves for instance:
  - Development or support in development of new methodologies;
  - Analysis, including very large data sets, through a range of modelling techniques and tools;
  - Insight and support to enhancement and development of representative scenarios;
  - Structured mission analysis (mission-to-task decomposition);
  - Application of OA techniques to facilitate decision making;
  - Provision of subject matter expertise (SME) across military and non-military domains, including reach to extensive networks of SMEs across NATO and in the nations;
- Analytic expertise in support of national Defence Planning activities, such as:
  - Education and mentoring with NATO analytic approaches;
  - Facilitation and delivery of customised Defence Planning studies;
  - Development, release, installation, in-service support, and customised enhancement of analytic supporting tools and models (e.g. the Joint Defence Planning Analysis and Requirements Toolset (JDARTS));

- Support to implementation of robust national capability-based planning processes;
- Exploitation of established NATO best practice, tailored to fit national needs;
- Facilitation of the use of NATO DP tools & models.

- **HQ Operations (peacetime & operational):** provision of tailored analytical support to tactical, operational and strategic-level HQs within Nations and the NATO Command and Force Structures, during peacetime and/or crisis situations. This support includes areas such as: planning; doctrine development; lessons identified; operational assessment; battle information management; data analysis (time-series, geospatial, survey), and streamlining of existing HQ data collection/analysis processes; implementation of advanced analytical techniques (mathematical modelling and optimisation algorithms); war gaming; etc. This support is available on-site (static or deployed locations) or as remote, reach back arrangement.

- **Information and Knowledge Management Requirements:** provision of analytical expertise to support the development and employment of Organisational IKM Policy, operational Information Management (IM) concepts, and the derivation and analysis of user's operational IM requirements. Broad and in-depth knowledge of the managerial value of relevant theories and current developments in the domain of IKM is applied to support areas such as:
  - Information use and knowledge mapping in organisations to recommend changes in structures, skills, processes and tools;
  - Information Exchange Requirements estimating;
  - Process, information flow, and scenario driven requirements modelling;
  - IM governance and policy Development;
  - Taxonomy and Maturity Model development and implementation.

- **Organisational Design and Improvement of Processes:** provision of expertise to lead or support a team conducting an organisational study in one or more of the following stages:
  - Analysis of the 'as-is' situation: stakeholder study, as-is process analysis, on-line staff questionnaires/surveys, analysis of current mission fulfilment, analysis of waste and duplication, identification of areas for improvement, etc.;
  - Provision of the 'to-be' structures or changes: development of organisational metrics, derivation and redesign of main processes, assessment of required skills and relative workload, simulation of HQ staff structures, assessment of the scale of the change management task, provision of statistical analysis of bids/gaps, etc.;
  - Option development and selection: the use of metrics and transparent multi-criteria decision analysis techniques to support auditable and evidence based decisions on structural changes.

- **Operational and User Requirements:** provision of expertise to support, through exploitation of products and knowledge from any of the other OA services, a range of areas including architecture development, CIS user requirements capture and validation, and mentoring in the utilisation of functional area services throughout their lifecycle.

- **NATO Concept Development:** provision of analytical expertise to support the development of concepts, including the conduct of qualitative and quantitative 'what if' analyses.

- **Problem Structuring:** provision of structured support to decision makers, helping them with identifying an agreed framework for their problem**.Service Flavours:** The OA service is tailored to meet individual needs of a customer.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost/ Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

SME008 - Standing Naval Forces CIS Operational Hand Over Service

Service ID: SME008

Service Name: Standing Naval Forces CIS Operational Hand Over Service (SNF CIS OHOS)

Portfolio Group: Subject Matter Expertise Service

Service Status: Pipeline

Service Description: The Service provides delivery, installation, configuration, and removal of SNF CIS Platform Services, as well as training of SNF Staff.

Value proposition: This service enables COM MARCOM to exercise C2 over maritime assets under MARCOM's operational control.

Service Features:

Planning: involves collaborating with MARCOM,SNF and the Host Nation (HN) of the oncoming maritime vessel; triggered upon MARCOM N6 staffing a Service Change Request at least one month before operational handover (OHO) is due to takes place (in exceptional circumstances 14 days) for each SNF OHO; site survey is a critical element of the planning process to facilitate a common understanding of the scope and capability of an SNF Platform service, to conduct a recce of the oncoming maritime vessel and to advise the Host Nation in their preparation to take on the SNF platform service;

Delivery: SNF CIS Platform equipment is delivered to a given location;

Installation: equipment is installed on the Identified Naval Vessel;

Configuration: End-to-end services (E2E) configuration;

Training: SNF Staff provided user training;

Removal: of the SNF CIS Platform equipment from the Identified Naval Vessel.

Service Flavours:

SNF CIS OHOS of SNF CIS Platform – Collocated Identified Naval Vessels: removal from and installation to an Identified Naval Vessel occurs at the same location immediately upon the removal from another Identified Naval Vessel;
SNF CIS OHOS of SNF CIS Platform – Non-Collocated Identified Naval Vessels: includes shipment of equipment and travel to the installation location upon removal of the equipment from an Identified Naval Vessel;
TACSAT/SEMARCOMM+ SNF CIS OHOS - Collocated Identified Naval Vessels: removal and installation of the specific TACSAT or SEAMARCOMM+ equipment set to an Identified Naval Vessel occurs at the same location immediately upon the removal from another Identified Naval Vessel;
TACSAT/SEMARCOMM+ SNF CIS OHOS – Non-Collocated Identified Naval Vessels: includes shipment of the specific TACSAT or SEAMARCOMM+ equipment set and travel to the installation location upon removal of the equipment from an Identified Naval Vessel.

Available on:

NATO Secret
NATO Unclassified
Non-Secure

Service Prerequisites:

MARCOM to ensure the Nations follow the latest MC195 Minimum Military Requirements

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is Per Handover. For price information per flavour, see the Service Rates document.

This page is left blank intentionally

APPLICATION SERVICES

V3.4

This page is left blank intentionally

APP001 - Specialist Application Service

Service ID: APP001

Service Name: Specialist Application Service

Portfolio Group: Application Services

Service Description: The Specialist Application Service provides technical support to all client facing specialist Commercial-off-the-shelf (COTS) applications approved by and available through the NCI Agency.

Value proposition: The Specialist Application Service provide applications that support a number of key activities that help allow a higher standard of work to be produced, making it easier and less time consuming for key individuals and teams to produce quality output.

Service Features: The Specialist Application Service provides ad-hoc technical support for COTS Application. This includes:

- Software lifecycle management;
- Infrastructure preparation for software deployment (Software Packaging);
- On Demand Software Deployment;
- Monitoring of Software licensed deployed

Service Flavours: The Service Flavours are based on the applications available and defined under the NCI Agency COTS Software Portfolio.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret

Service Prerequisites:

WPS001 - Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP002 - SEW Application Service

Service ID: APP002

Service Name: SEW Application Service

Portfolio Group: Application Services

Service Description: The SEW (Shared Early Warning) Application Service provides the user with NATO's 24/7 early warning capability to disseminate Tactical Ballistic Missile (TBM), provided by US national capabilities, to NCS HQs, NATO HQ and political representatives in NATO nations.

Value Proposition: The SEW Application Service provides standardised NATO warning and situational awareness of ballistic missile threat launches to support situation awareness, high-level political and military consultation and decision making.

Service Features: The SEW Application Service provides visual and audio alerts when each ballistic missile launch is reported. Also, the SEW application service visualizes the reported launch and predicted impact points on map displays. Past missile launches can be reviewed, including key data on threat characteristics.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP006 - Ballistic Missile Defence (BMD) Application Service

Service ID: APP006

Service Name: Ballistic Missile Defence (BMD) Application Service

Portfolio Group: Application Services

Service Description: The Ballistic Missile Defence (BMD) Application Service provides functions that enable NATO to integrate sensor information, build and distribute a comprehensive and real-time BMD operational picture, and exercise command and control of voluntary national contributions (sensors and effectors) provided by Allies. The application TMD Air Command and Control System (ACCS TMD1) is the core integrator of the BMD functions.

Since the Service is considered as a System of Systems (SoS), it comprises a set of dedicated work positions enabling users to operate BMD. Other services, contributing to the Service are:

- APP061 Air Command and Control Information System (Air C2 IS)
- APP007 Tool for Operational Planning Functional Area Service (TOPFAS)
- APP022 NATO Common Operational Picture (NCOP)
- INF025 Deployable Communications and Information systems (DCIS)
- INF002 - NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (NATO to Nation Gateway [NNG]):
- APP010 Networked Interoperable Real-time Information Services (NIRIS)

The actual service composition depends on the customer's operational requirements and it is configured individually in close cooperation with the customer.

All above listed services operate on the NATO General Communications System (NGCS) network. National feeds are provided through NATO-National static gateways or through NATO deployable CIS equipment. NCI Agency Air and Missile Defence Command and Control (AMDC2) Directorate owns the functions provided for BMD and it operates the Service, with relevant contributions and support from various other NCI Agency Directorates or their Service Lines.

The Service is still under development and therefore has yet to reach its final operational capability.

Value Proposition: The aim supported by the Service is to achieve full coverage and protection for all NATO European populations, territory and forces against the increasing threats posed by ballistic missiles. This also includes required protection of deployed forces and high value assets/areas within an area of operations/interest from attacks by ballistic missiles. BMD interlinks all levels of military command from the military strategic down to the tactical level all across the Alliance regardless of the country or the respective military service. BMD is a fully combined and joint service.

Service Features: BMD related features are:

- Situational awareness;
- Planning (including simulation) and tasking;
- Execution and monitoring;
- Early warning of missile launches;
- Threat analysis; and
- Reporting.

Service Flavours: TMD has static and deployable components, depending on the operational use of BMD.

Available on:

NATO Secret

Service Prerequisites:

BMD relies on an infrastructure able to host the TMD application and the relevant and dependent services. Enabling intra and inter-site data exchange through networking services.

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP007 - TOPFAS Application Service

Service ID: APP007

Service Name: Tools for Operations Planning Functional Services (TOPFAS) Application Service

Portfolio Group: Application Services

Service Description: TOPFAS (Tools for Operations Planning Functional Services) Application Service provides the user with integrated collaboration planning and decision support capabilities. This service is comprised of multiple modules that support Systems Analysis, Operational Planning, Execution and Assessment of Operational Campaigns. This service also supports the force generation management process and offers ORBAT (Order of Battle) service.

Value Proposition: TOPFAS Application Service offers the user (through the suite of available modules) a distributed, multi-level and a collaborative environment that benefits standardization, productivity and quality to operational planning processes.

Service Features: The TOPFAS Application Service is comprised of the following modules:

- Systems Analysis Tool (SAT) – Supports systems analysis of the engagement space for holistic situational awareness and understanding.
- Operations Planning Tool (OPT) – Campaign planning tool that supports the development and synchronization of strategic options, operational and tactical courses of action
- Campaign Assessment Tool (CAT) – Supports measuring progress towards the planned campaign end-state.
- ORBAT Management Tool (OMT) – supports building and viewing order of battle (ORBAT) information and allows for management of national and NATO Response Force (NNRF) ORBATs.
- TOPFAS Web Portal (TWP) – Provides TOPFAS information content to be shared with wider communities of interest through an internet portal
- User Management Tool (UMT) – Allows TOPFAS administrators to manage user access and roles

Service Flavours: TOPFAS Application Service is available in the following flavours:

- Flavour 1: 1-50 Users
- Flavour 2: 51-300 Users
- Flavour 3: 301-1000 Users
- Flavour 4: 1001 Users +

Available on

NATO Secret

If you require availability of any other security domain please raise this as a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP010 - NIRIS Application Service

Service ID: APP010

Service Name: NIRIS Application Service

Portfolio Group: Application Services

Service Description: The NIRIS (Networked Interoperable Real-Time Information Service) Application Service provides situational information in support of automated (Air) C2 and information systems within NATO. NIRIS Application Service does this through the enablement of data collection, dissemination and transformation of information in an interoperable manner, based upon NATO and Commercial standards.

Value Proposition: The NIRIS Application Service is integral for communities of interest within Air, Land, Maritime, Joint, Logistic and Intelligence domains. NIRIS Application Service acts as a middle layer between data producers and information consumers (e.g. systems to include iGeosit and NCOP) making information collected from multiple sources available to decision makers (via service) as Battle Space Objects (BSO).

The key values of NIRIS are:

- Provision of (near) real-time situational awareness for operations.
- Wide range of supported interfaces for data collection and exchange strongly supporting interoperability.
- Harmonised view via BSO's on the collected data with access to in-depth detail to support decision makers.
- Allows integration via several standardised interfaces with other NATO and National systems.

Service Features: The NIRIS Application Service features the ability for data collection, dissemination and transformation of data in an interoperable manner based on NATO and commercial standards. Furthermore, it provides services to perform data format conversions, recording/replay and track augmentation.

A key feature is the versatility of is interoperability. The main supported interfaces for data collection and exchange are:

- Link1 (STANAG 5501) – Air Picture
- Link 11B (STANAG 5511) – Maritime, Air Picture
- Link 16 (STANAG 5516) – Air, Ground, Maritime, BMD Picture (and more)
- JREAP (STANAG 5518) – Transport for Link 16
- VMF (STANAG 5519) – Ground Picture
- Link 22 (STANAG 5522) – Maritime, Air Picture
- OTH-Gold – Maritime, Ground, Air Picture
- NFFI ("D" Doc) – Friendly Force Tracking (Ground) Picture
- FFI-MTF-XML (STANAG 5527) – Friendly Force Tracking (Ground) Picture
- SIMPLE (STANAG 5602) – Transport for Link 11, Link 16, Link 22 (for IO testing)
- ITV and VATS – Civilian Convoys
- Automatic Identification System (AIS) – Civilian Maritime Picture
- Eurocontrol ASTERIX (including ADSB) – Civilian Air Picture and Air Traffic Control

The main supported interfaces for data and information consumers are:

- Trackstore integration (via API) –Provision of (near) real-time BSO information
- NVG (NATO Vector Graphics) – BSO overlays via web-services
- KML (Keyhole Markup Language) – BSO overlays via web-services
- SIP3 – Friendly Force Tracking information via web-service interface (NFFI, FFI)

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret
Availability on any other security domain is TBC upon a New Service Request.

Service Prerequisites:

SEC011: Security Certificate Service

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP011 - OANT Application Service

Service ID: APP011

Service Name: OANT Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The OANT (Online Analyser for Networked Tactical-Data) Application Service provides the user with a quick and easy way to analyse C4ISR data flowing on operational, test and/or exercise networks. OANT Application Service provides compliancy reports to agreed NATO Standards, plus providing Revision, Extract and Report capabilities on the logical connectivity of the data flows. Furthermore the provision of capability in the checking of data quality.

The OANT Application Service provides a both a thick client (OANT SWING) and a web-based net-enabled service (OANT WEB) interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols, such as: JREAP, GMTI, Link 16, Link 11, Link 1, NFFI, FFI, DIS and OTH-G.

Value proposition: The OANT Application Service provides its users with the following number of key benefits:

- NATO Standardization and Standards V&V bodies: test and verify quality and improve content of STANAGs for completeness, correctness, ambiguities and vagueness.
- War fighters (J3 and J6): up-to-date web access to shared assessments and improved situational awareness of data flows, connectivity and exchanged data quality, increasing trust in the information used to support decision making.
- OPS and interoperability event network, service management and control and analysis groups: smarter, improved and shared means of monitoring connectivity and data quality, to identify, understand and troubleshoot data and interoperability issues in a timely manner.
- System/Service developers: cost and time-savings with improved insight into STANAG compliancy and data content of exchanged messages to support self-analysis and continuous “pretesting” in order to foster out-of-the-box plug-and-play interoperability.

Service Features: The OANT Application service is comprised of the following features:

- Enablement of one-to-one mapping between Standard Specifications and the way OANT interprets messages, words and fields
- Interpretation of received messages from bits and bytes into human readable information
- Assessments of received message contents against applicable standards leveraging on XML generated metadata and data specifications captured in-line with the STANAG/Standards Transformation Framework (STF) Design Rules (NISP, 2014)
- Collection and reporting of statistics on received data (including but not limited to breakdown per payload format, message originator, message label and encountered error type)
- Provision of further insight in to derived message information (e.g. track information)
- Interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols, such as JREAP, GMTI, Link 16, Link 11, Link 1, Link 22, VMF, SIMPLE, NFFI, FFI, DIS and OTH-G.

In addition, the OANT-WEB service flavour offers the following features: provision of analysis and verification of a data forwarding process; comparing both the input the stream and the forwarded data stream; and providing an assessment of whether the forwarding occurred in accordance with the applicable data forwarding standard.

Service Flavours:

OANT SWING – a thick client application run on a workstation
OANT WEB – designed to be deployed in a distributed environment

- OANT Web flavour is required in order to be able to provide data to the SMACQ Application Service for further analysis of data connectivity, timeliness and quality, to provide an aggregated and historical view on these measurements collected from various sources.
- SMACQ and OANT together form the C2 IOTA (C2 data Interoperability & Traffic Assessment) Services Suite.

Available on:

NATO Unclassified
NATO Secret
Mission Secret
The Service may be available on other networks upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost/ Price: The Service unit of measure is Per Site.

APP012 - SMACQ Application Service

Service ID: APP012

Service Name: SMACQ Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The SMACQ (Service to Monitor and Assess Connectivity and Quality) Application Service provides the user with capability to monitor data exchange of operational information dissemination networks to assess and report on its logical connectivity and quality based on Standards. SMACQ leverages and combines information obtained from OANT (APSC209) and/or NIRIS (APSC209) Application Services, to provide further analysis of data quality KPIs, such as connectivity, timeliness, activity and compliancy, insights on historical trends and changes of these KPIs via statistical reports and an overall aggregated graphical view via simple traffic colour-coded indicators.

Value Proposition: SMACQ Application Service offers the following key benefits for a wide range of users including but not limited to following:

- Commanders, as SMACQ is monitoring and reporting on the full data flow quality, it provides Decision-makers with an enhanced situational awareness and higher increase in the trust on the data they are using to make more effective decisions.
- War fighters (J3 and J6), usually having an isolated, localized view of their data flows, but typically unaware of flows of external data sources, are now able to share a common picture of the data quality, logical connectivity and timeliness of the operational data flow among the battlespace capabilities. SMACQ provides access to simple traffic colour-coded indicators on the systems and services they use, via toggle-able geographical overlays, to improve their situational awareness and trust in the data they are sharing and receiving, so they can be more assured in how they use that data.
- OPS Service Management and Control, SMACQ provides up-to-date web access to the same shared common picture that the war fighters are seeing, with more detailed assessments of the data and connectivity quality indicators, enabling smarter, improved and shared means of monitoring, reporting on connectivity and data quality from source to consumer, to identify, understand and troubleshoot issues in a timely manner.

Service Features: According to the Bi-SC Operational Requirements for the NATO Common Operational Picture (COP), if the source quality of information data is available, then this shall be accessible to COP users.

SMACQ Application Service provides the following three enhancements to the NATO Common Operational Picture (COP) and Recognized Pictures (RPs) through a toggle-able geo-graphical overlay to the COP/RPs accessible via standardized interfaces (e.g. NVG, KML):

- **Source Quality**–SMACQ provides knowledge about the source quality, based on Standards-compliance, and potential degradation of the quality for various data flows. For example, the quality of tracks and/or messages generated by a source could be indicated by traffic-light colour-coded dots overlaid on the reported tracks and sources.
- **Source Activity**–SMACQ provides knowledge about the source activity and how much time had elapsed since that source reported on particular tracks. This is indicated by traffic-light colour-coded lines linking the reported tracks to the sources.

- **Source Connectivity**– from analysing the data flows from multiple points, the information about a source's logical connectivity, from source to consumer(s), can be inferred and/or extracted, and this information made available to the COP. The source connectivity per source are provided as lines connecting the monitored points from source to consumer(s).
- **Data Timeliness**– by analysing the data flow activity at each monitored point, the information about data timeliness is also made available to the COP. The data timeliness per connection are indicated by traffic-light colour-coded lines connecting each of the monitored points from source to consumer(s).

Service Flavours: The SMACQ Application Service can be offered as a single stand-alone decentralized application service or as a centralized hosted service.

- A centralized hosted SMACQ service can provide insight into an enterprise-level operational network, such as NATO Static Command, to monitor and assess data flows.
- A separate SMACQ application service may provide run-time support during missions and exercises or in a federated-environment, providing localized assessment of those networks, as needed.

Available on:

NATO Secret
Mission Domain
PAN
The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The Service unit of measure is Per Instance.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP013 - IEG-FS Application Service

Service ID: APP013

Service Name: IEG-FS Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The IEG-FS (Information Exchange Gateway for Functional Services) Application Service provides functional service proxies (FAS Proxy) that support Information Exchange Gateway (IEG) solutions to enable cross-domain exchange of operational data (e.g. Chat, TDLs, JISR, Air, Land, and Maritime). IEG-FS can support IEG-B and IEG-C scenarios (NATO Secret to NATO-Nation Secret enclave, and NATO Secret to NATO-led Mission Secret enclave [reference ADaTP-34 NC3TA Vol. 2 v7, 2005]), which are the most relevant for NATO and partner nations.

Value Proposition: Effective operations require the exchange of a wide variety of data within and between Command and Control (C2) systems. The traditional approach to multi-security-domain networking, forbids most information flows crossing the boundary of the security domain. This restrictive approach results in serious limitations to the information exchange requirements among C2 entities. Cross security domain services mediate in any information exchange occurring between the different information domains and levels of classification. The IEG-FS Application Service provides the user with the integration of both Tactical data Link and chat services between distinct security domains, while protecting information assets of the participants in a federated environment.

Service Features: The IEG-FS Service is designed to extend an IEG for Core Services (such as email or web browsing) with extra functionality (in this case with Functional Services). The purpose of IEG-FS are:

(1) Label – determine and mark the security classification of information passing the IEG, in order to ensure that the information reaches the intended audience,

(2) Sanitize the information that is intended to leave the security domain. This sanitization will happen according to rules, and it removes or modifies data contents in order to be able to release functional services data into another domain,

(3) Sign – ensure that data or its security classifications are not changed, by adding digital signatures to the data, when converting data to XML format,

(4) Verify and guard – ensure the validity of the data by verifying adherence of data to the applicable standards or STANAGs (e.g. STANAG 5516 for Link 16 or XMPP standard for JCHat) both when entering the IEG and when exiting it. Invalid data will not pass the IEG.

The IEG-FS supports multiple formats and protocols, including within the Tactical Data Link (TDL), Message Text Format (MTF), and Chat (XMPP) domains.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP014 - NMRR-VMS Application Service

Service ID: APP014

Service Name: NMRR-VMS Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The NMRR-VMS (NATO Metadata Registry & Repository - Vocabulary Management Service) Application Service provides a consistent, controlled and reliable means to store, manage and access XML artefacts, including code lists, metadata and data specifications. It facilitates the configuration management, quality management and change control of registered specifications, as well as enables controlled search, retrieval and dissemination of those artefacts.

The VMS interface allows the standards and data managers a tool to support metadata and data harmonization and mapping across multiple technical communities

The NMRR-VMS provides both a business-to-business service and web-based interface.

Value Proposition: The NMRR-VMS Application Service is an essential component in the implementation of the NATO Network Enabled Capability (NNEC) Data Strategy, acting as an enabler for realization of the Federated Mission Networking (FMN) and Connected Forces Initiative (CFI).

Key benefits of the NMRR, as an Enabling Service, is in creating an environment that provides improved situational awareness to the Warfighter via:

- Flexible, centralized, authoritative controlled updates, notifications and access to run-time changes to code lists, security policy information files, and other relevant registered artefacts
- Enhanced data interoperability between anticipated and unanticipated users in the service oriented environment, realized via the provision of visibility and accessibility to the controlled set of registered XML metadata and data specifications to all systems/services.
- Dynamic configuration management, quality management and change control of registered specifications, thus enabling improvement of the standardization process and compliance of systems with the standards
- Semantic-based and standardized data harmonization, across multiple communities, offering a view on the information semantic adopted inside the communities and providing the possibility to relate similar concepts.

Service Features: The NMRR-VMS provides both a business-to-business service and web-based interface to enable controlled registration, discovery and access to:

- XML artefacts (e.g. XML, XSD, RDF, OWL, Schematron)
- STF-aligned metadata and data specifications (e.g. Link16, ADatP-3, IPIWG, FDMS)
- Run-time codelist and allowable value lists, SPIF
- Service Descriptions (e.g. WSDL)

The NMRR-VMS acts as a Metadata Repository of XML artefacts, as recommended by the XML Management Services Working Group (XMLSWG) and approved by the Information Services Subcommittee (ISSC). It supports the NATO Discovery Metadata Specification (NDMS) as the specification for its metadata cards.

- The NMRR-VMS provides the user with the capability to facilitate the configuration, quality management and change control of registered specifications, as well as enables the access-controlled search, retrieval and dissemination of those artefacts.

The NMRR-VMS also acts as a Metadata Registry for the contents defined within the metadata and data standards, leveraging on the specifications captured in-line with the STANAG/Standards Transformation Framework (STF) Design Rules (NISP, 2014). The STF-aligned specifications enables the machine-processability and standardized interpretations of the specifications.

- The latter capability provides access to the contents of the XML artefacts, including the namespace and vocabulary (data elements, value lists, etc.), enabling a more efficient and effective XML namespace, metadata and data management across multiple communities of interest (COIs). Furthermore, the VMS interface allows the standards and data managers a tool to support metadata and data harmonization and mapping across multiple technical communities, and enables run-time value and code list management to support dynamic, interoperable semantic-based information exchanges.

Finally, the NMRR-VMS supports the Federated Registries concept, enabling the creation and joining to a federation of registries. This enables issuing a query against a single logical metadata registry, which returns the union of corresponding metadata from all registries in the federation. This supports and enables the NATO FMN Implementation Plan.

Service Flavours: The NMRR-VMS Application Service is available as:

- The centralized hosted NMRR-VMS service provides development-time support to standardization body members under the NATO C3 Board (C3B).
- A separate NMRR-VMS application service may provide run-time support during missions and exercises, providing a central repository for code lists and processing rules.

Available on:

NATO Unclassified
The Service may be available on other security domain upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] Target: 98.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Support Hours: Support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time) via e-mail on: nmrr@ncia.nato.int

Service Requests:

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Incident/problem reporting:

Via e-mail to nmrr@ncia.nato.int

New Service Request:

To request access to the NMRR, register as a user via the NMRR internet facing web application https://nmrr.ncia.nato.int/

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP015 - JCHAT Application Service

Service ID: APP015

Service Name: JCHAT Application Service

Portfolio Group: Application Services

Service Description: The JCHAT (Secure Tactical Joint Chat) Application Service provides the user with a federated chat network to allow near real-time communication, or semi-synchronously via text messages, between two users, ad-hoc groups and within persistent chat rooms.

Value Proposition: The JCHAT Application Service is a key component in facilitating military effectiveness. It enables passing of information, coordination of operations and support to collaborative decision making. The service focuses on time critical operations in order to prevent casualties and minimise reaction time.

Service Features: The JCHAT Application Service key features, include but are not limited to:

- Multi-party messaging service (ad-hoc and persistent chat rooms)
  - Within a mission network, chat applications are used in a similar manner to Combat Net Radio, allowing all-informed exchange of information within specific groups or chat rooms.
  - Chat rooms are used both informally, for staff level coordination and collaboration, and formally, for rapid all-informed reporting and tasking.
- One-to-one messaging service (chat sessions)
  - Presence and instant messaging (IM) defines a method by which a client or user can formally request establishment of a presence and instant messaging session.
  - The functionality of the JCHAT Application Services follow open standards and are set in conformance with the requirements in RFC 2779 ("Instant Messaging / Presence Protocol Requirements").
- Roster service (contact list)
  - In JCHAT, a user's roster contains any number of specific contacts. A user's roster is stored by the user's server on the user's behalf so that the user can access roster information from any device.
  - Because the user's roster can contain confidential data, the JCHAT server restricts access to this data so that only authorized entities (typically limited to the account owner) are able to retrieve, modify, or delete it.
- Presence service (logged-on users)
  - The concept of presence refers to an entity's availability for communication over a network. At the most basic level, presence is a boolean "on/off" variable that signals whether an entity is available or unavailable for communication (the terms "online" and "offline" are also used).
  - In JCHAT, presence typically follows a "publish-subscribe" or "observer" pattern, wherein an entity sends presence to its server, and its server then broadcasts that information to all of the entity's contacts who have a subscription to the entity's presence. A client can establish a "presence session" at its server by sending initial presence, and where the presence session is terminated by sending unavailable presence.

Service Flavours:

- Single, standard version based on NCI Agency prototypes

- Single, standard version based on Commercial Off the Shelf (COTS) software
- Clustered dual-node multi IM domain version based on COTS software
- Single, deployable version for mobile units based on COTS software
- Cross-domain chat version based on NCI Agency prototypes

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Device Service
SEC011 – Information Exchange Gateway

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP016 - JTS/FAST Application Service

Service ID: APP016

Service Name: JTS/FAST Application Service

Portfolio Group: Application Services

Service Description: The JTS/FAST (Joint Targeting System/Flexible, Advanced C2 Services for NATO Time-Sensitive Targeting) Application Service provides the user with capabilities to provide integrated joint objective and effects-based targeting, campaign synchronisation, target development, target list management, target folder preparation, target imagery management and battle damage assessment.

Value Proposition: The JTS/FAST Application Service, used throughout all command levels in NATO (both static and deployed) as well as nationally by various nations, enables collaboration and the efficient and timely exchange of critical information in support of the Joint Targeting process Furthermore this service is designed to aid tracking and prosecuting of Time-Sensitive Targeting (TSTs).

Service Features: The JTS/FAST Application Service contains two main end user modules, with distinct features:

- JTS features:
  - Deliberate Targeting
  - Kinetic and Non-Kinetic Targeting
  - Effects-Based Targeting (JFX)
  - High Value Individual (HVI)
  - Target Development
  - Target Folder Preparation
  - Objective Management
  - Target List Management
  - Target Nomination Process
  - Target Media Management
  - Weaponing Solutions
  - Battle Damage Assessment (BDA)
  - Campaign Synchronization
  - ATO Planning Cycle
- FAST features:
  - Dynamic Targeting (DT)
  - Time-Sensitive Targeting (TST)
  - Integrated Chat capability
  - Integrated Map functions
  - Network-enabled, real-time coordination

Service Flavours: The service is available as the following flavours**.**

JTS/FAST Software

Includes all JTS/FAST software components and documentation to have either a full JTS/FAST site (server and clients) or JTS/FAST client workstations which would be able to remotely connect to a full JTS/FAST site.

JTS/FAST Capability

Includes the JTS/FAST software, documentation, platform and database binaries for building a full JTS/FAST system with the full set of functionality provided by the JTS/FAST server and client.

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP017 - LC2IS Application Service

Service ID: APP017

Service Name: LC2IS Application Service

Portfolio Group: Application Services

Service Description: The LC2IS (Land C2 Information Systems) Application Service provides a suite of functional modules to support operational land staff in the execution of their operational missions, processes and tasks. The LC2IS Application Service functionality is delivered through three main components: web portal desktop application, Desktop, and Web application. This service allows for the sharing of information and provides interoperability between other NATO functional services and National Land C2 systems.

Value Proposition: The LC2IS Application Service offers the user shortened Information Decision Action (IDA) cycles, inherent to Command and Control mission executions. This service enables:

- More effective, efficient and accurate management of Recognized Ground Picture (RGP)
- Improved sharing of data, information and knowledge
- Improved support for operations planning and FRAGO production
- Enhanced NATO Situational Awareness
- Increased time saving through automated importing of RGP contributions, briefings and message imports and generation

Service Features: The main service consists in the provision of the LC2IS Application, comprising three main components:

- **Web Portal, supporting**:
  - Node administration/configuration, (role-based) access management
  - Information sharing (private or shared workspaces) and general situation awareness
  - Interoperability configuration (e.g. MIP)
- **Desktop Application (DA. otherwise called "Thick" client), supporting:**
  - (geo-based) Situation Awareness
  - Battlespace Object and Battlespace Control Measure management
  - Command and Control, e.g. fragmented orders, import and export of standard messages)
- **Web Application:**
  - (geo-based) Situation Awareness
  - Simplified Battlespace Object Management

Optional services include installation, on-site and remote support, testing, training, mentoring and analysis/evaluation.

Service Flavours: Based on the configuration, the Service has the following flavours:

A. Availability: (1) High (redundant DB Service) or (2) Low (not redundant DB Service)
B. Friendly Force Track Injection: (1) Supported or (2) Not Supported
C. (1) Operational/Exercise or (2) Training Configuration
D. Message Processing: (1) Minimal or (2) Full
E. Autonomy: (1) Autonomous (on a stand-alone managed device) or (2) Standard

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP018 - MCCIS Application Service

Service ID: APP018

Service Name: MCCIS Application Service

Portfolio Group: Application Services

Service Description: MCCIS, (Maritime Command and Control Information System) Application Service, processes electronically data from multiple sources and displays information in various command and control applications. The MCCIS Application Service adds visualisation of information in a high resolution map covering large areas without losing detail. It provides military users with naval operational data in a multi-national environment through Over the Horizon Targeting (OTH-T)-GOLD and Allied Data Publication No 3 (ADatP-3) messages. The MCCIS Application Service provides capabilities to acquire and manage C2 situational awareness data. The system is built around hardware and a software environment based on industry standards and widely accepted components. The MCCIS application service and community contribute a high quality Recognized Maritime Picture (RMP), Recognized Air Picture (RAP) and Recognized Grand Picture (RGP) to NATO's situational awareness and Common Operational Picture.

Value Proposition: The MCCIS Application Service offers the user to visualise, transmit and share Maritime C2 related information. MCCIS Application Service supports planning and controlling naval operations, and provides the Recognized Maritime Picture (RMP)., as well as maritime operations data such as naval mission planning, naval mission reporting, situational awareness, and resource management and intelligence. This enables naval commanders and staffs to automatically receive, analyse, display, and manipulate data, while supporting more accurate, timely decisions.

Service Features: The MMCIS Application Service offers the user network services (Email, Chat, Net Meeting), Web Information Service Environment capabilities (WISE), access to databases, Operational Applications and Web Page Development. The MMCIS Application Service features maritime operations data, including but not limited to, naval mission reporting, situational awareness resource management and intelligence.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP019 - MSA BRITE Application Service

Service ID: APP019

Service Name: MSA BRITE Application Service

Portfolio Group: Application Services

Service Description: The MSA (Maritime Situational Awareness) BRITE Application Service, based upon on Baseline for Rapid Iterative Transformational Experimentation (BRITE), provides the user with a diverse web based set of integrated command and control features, compatible with NNEC tenets. MSA BRITE is deployed to HQ MARCOM as an operational prototype. It is used in support of maritime operations such as Active Endeavour, Ocean Shield and Unified Protector.

Value Proposition: MSA BRITE Application Service benefits the NATO Shipping Centre in MARCOM to support operations in a non-military environment, such as illegal movement of products and people. The capabilities of this service, together, allow the NATO Shipping Centre at MARCOM to produce the Recognised White Shipping Picture. The merchant shipping picture equivalent of the Recognised Maritime Picture.

Service Features: The MSA BRITE Application Service provides the viewing of a Recognised Maritime Picture (RMP) for 'White Shipping' through service ingesting information from National, Industrial and Open Sources. This service features:

- Display and analysis capabilities for civilian maritime traffic
- Information collection from open sources to compile the White Picture
- Automatic anomaly detection provided by various smart agents activated by operators

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
NATO Unclassified

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP020 - iGeoSIT Application Service

Service ID: APP020

Service Name: iGeoSIT Application Service

Portfolio Group: Application Services

Service Status: Retired

Service Description: The iGeoSIT (NATO Interim Geospatial Situation Intelligence Tool) Application Service provides the user current geospatial intelligence information that can be used to access and visualise operational information from NATO theatres anywhere within the network. On NATO Command Structure and NRF networks, the NCOP application service has been replacing iGeoSIT application service since 2015 (NCOP FSA).

Value Proposition: The iGeoSIT Application Service offers, through Geospatial Awareness, enables support to horizon scanning, area of interest monitoring, Crisis Monitoring, Crisis Response and Mission Execution.

Service Features: The iGeoSIT Application Service features an intuitive graphical user interface from which you can access, in real time, geospatial datasets (maps, satellite imagery) and operational data (e.g. mine situation reports, bridge information, etc). The iGeoSIT Application service features interoperability for operational data; includes standard databases, NATO Vector Graphics and KML. Geospatial data is served using the standard OGC WMS interfaces.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP021 - JOCWatch Application Service

Service ID: APP021

Service Name: JOCWatch Application Service

Portfolio Group: Application Services

Service Description: The JOCWatch (Joint Operations Centre Watch) Application Service provides the user with a web-based electronic event log. The JOCWatch Application Service provides support to Watch Keepers and Shift Directors within Operation Centres (CJOC, JOCs, etc.) to record and disseminate incident information in a standardised and structured manner. It also provides an audit trail (a legal log) of all incidents related to an operation.

Value Proposition: The JOCWatch Application Service offers a common web-based interface which allows Operations Centre staff to manage, analyse and publish information on incidents. Through provision of event-data for analysis of the battle-space this service enables greater situational awareness for decision makers from subordinate commands to their HQ.

Service Features: Functionally JOCWatch Application Service offers a web based interface to:

- Capture and publish incident information,
- RSS Feed alerting of incident updates
- Search and audit capabilities,
- Compatibility with KML (show of incidents in Google Earth)
- NATO Vector Graphics web services (Map overlaying).
- Dashboard reporting (providing an immediate overviews of situations).
- Interoperability with multiple NATO and National Systems (e.g. LOGFAS, iGeoSIT, CC).

Service Flavours: The JOCWatch Application Service is in the following flavours:

1. Standard offering
2. Federated offering – all standard features, with the addition of reporting functionalities through chain of commands or across multiple missions

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP022 - NCOP Application Service

Service ID: APP022

Service Name: NCOP Application Service

Portfolio Group: Application Services

Service Description: The NCOP (NATO Common Operational Picture) Application Service provides operational user with a common view of the battle space with forces and partners. The NCOP Application Service is interoperable to a large set of standard or dedicated interfaces (through which NCOP obtains various authoritative data sources) allowing the user to build the most complete Common Operational Picture tailored for the mission.

Value Proposition: The NCOP Application Service offers the user situational awareness based upon information received from various NATO and National Systems, collating and harmonizing this information into mission-tailored Common Operational Pictures (COP), thus making required information available to NATO force audiences in a timely and responsive manner so they may execute their own processes (Battlespace Management, Logistics, Targeting, MEDEVAC, etc).

Furthermore, the NCOP Application Service also contributes to the Ballistic Missile Defense capability through integration of specific functions and interfaces for BMD.

Service Features: The NCOP Application Service offers the user a mission-tailored Common Operational Picture through interoperability and COP management capability, including a web-access capability (Geo COP Editor) and the dissemination of web services to other Functional System. The NCOP Application Service features tailoring capabilities to represent and exploit information in various manners, and a management tool in which to control and disseminate COP to different commands.

The NCOP Application Service features also interoperability techniques to obtain information products for the COP from various XML, structured format and OGC compliant authoritative data sources.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP023 - NAMIS Application Service

Service ID: APP023

Service Name: NAMIS Application Service

Portfolio Group: Application Services

Service Description: NATO Automated Meteorological Information System (NAMIS) Application Service provides a sustained NATO Meteorological and Oceanographic (METOC) application functionality for the NATO. NAMIS Application Service provides direct weather support to NATO-led operations by providing coherent, comprehensive, and harmonised weather information and products throughout ACO activities.

Value Proposition: The NAMIS Application Service delivers METOc information to its users, principally within two Communities of Interest groups; MetOc and Ops Communities. NAMIS Application Service enables the user to access raw MetOc data and able to produce MetOc observations. Those can be used to support Exercise or Operation planning, Navigation, Natural Hazard Prevention/Analysis, Logistic Support Planning, Air/Missile Defence Operation planning/analysis, Weather Forecast Impact Analysis purposes. Users can also visualise all available MetOc products and data via NAMIS. Thus, interoperability of weather systems and other FAS is enabled.

Service Features: The NAMIS Application Service provides below listed features:

- Provision of Environmental Information Products,
  - MetOc Data Distribution System
- Meteorological Assessment,
  - visualization of forecasts,
  - visualization of observations,
  - visualization of value added products such as satellite images,
  - management of information on meteorological stations
- Tactical Specialist Tools,
  - Meteorological messages for CBRN (EDM and CDM),
  - Ballistic Wind Messages,
  - Color state and forecast trend for user selected airfields (METWATCH),
  - Products supporting parachute operations Mean Effective Dropping Wind (MEDW), Surface Wind and Gusts (SFG),
  - Theatre Crosswind Monitor, to monitor selected airfield for crosswind threshold,
  - Density Altitude calculator to verify conditions for use of air assets on the specific areas,
  - Graphical depiction of "Human Exposure", including Temperature-Humidity index (Heat Stress), Wind-Chill, Cold-Water Survival,
  - Night Illumination.
- Operational Planning Support (meteorological briefs in support of operations);
- Meteorological briefs in support of operations.

Service Flavours: The NAMIS Application Service is available as three flavours; namely:

- NAMIS X Premium; Superior license type providing full suite of full MetOc analysis tools
- NAMIS Basic; junior license type providing access to limited MetOc analysis capability
- NAMIS 'NATO MetOc (NMD) Web Portal providing access to…MetOc information

Available on:

NATO Secret
NATO Unclassified
Mission Domains

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP025 - MCM EXPERT Application Service

Service ID: APP025

Service Name: MCM Application Service

Portfolio Group: Application Services

Service Description: The MCM EXPERT is a tool used for planning Naval Mine Counter Measure (MCM) operations to achieve user-specified level of clearance of maritime channels through uniform and non-uniform coverage according to the doctrine stipulated in STANAG 1454.

Value Proposition: The MCM EXPERT Application Service offers the user a Graphical User Interface (GUI) for interactive planning of MCM operations. Different inputs (matching different MCM operation types) are required from the user and a quick response is given in the form of a set of minesweeping or mine hunting tracks, with specific placement across the channel, and the clearance and remaining risk level achieved after completion of the given plan.

Service Features: The MCM EXPERT tool provides the ability to build Uniform and Non-Uniform plans based on level of clearance, remaining risk, and Non-Uniform plans for time-constrained operations. Metrics of clearance, and remaining risk, achievable with the selected plan presented to the user.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP026 - Virtual Battle Simulation (VBS) Application Service

Service ID: APP026

Service Name: Virtual Battle Simulation (VBS) Application Service

Portfolio Group: Application Services

Service Description: The Virtual Battle Simulation (VBS) application service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space at the level of detail of individual actors with a degree of realistic visualisation.

The VBS application is a commercial-off-the-shelf immersive training application used to simulate a real-time video stream. It functions as stand-alone or connected to the JCATS model.

Value Proposition: This application service supports exercise designers and control organisations in generating life-like visualizations of the relevant battlespace.

Service Features: The Virtual Battle Simulation (VBS) application service offers the following features:

- Creation and modification of a virtual scenario including terrain, systems and personnel. Activities of systems and personnel can be pre-planned and previewed.
- A player and controller mode to execute the scenario and act as one the parties or as the scenario manager.
- Video capture to mimic the behaviour of real-time optical or infra-red sensors.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability
Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP027 - NATO Nuclear C2 Reporting Application Service

Service ID: APP027

Service Name: NATO Nuclear C2 Reporting Application Service

Portfolio Group: Application Service

Service Description: The Service is classified. Further information is available upon request and relevant clearance.

Value proposition: -

Service Features: -

Service Flavours: -

Available on: -

Service Prerequisites: -

Standard Service Support Levels: -

Service Cost / Price: -

The Service is classified. Further information is available upon request and relevant clearance.

APP028 - NATO Nuclear Planning Application Service

Service ID: APP028

Service Name: NATO Nuclear Planning Application Service

Portfolio Group: Application Service

Service Description: The Service is classified. Further information is available upon request and relevant clearance.

Value proposition: -

Service Features: -

Service Flavours: -

Available on: -

Service Prerequisites: -

Standard Service Support Levels: -

Service Cost / Price: -

The Service is classified. Further information is available upon request and relevant clearance.

APP029 - Military Message Handling Application Service

Service ID: APP029

Service Name: Military Message Handling Application Service

Portfolio Group: Application Services

Service Description: Military Message Handling Application Service provides the user, in both static and deployed environments, with the capability of drafting, releasing and receiving military messages (ACP127). The service also delivers a reliable message storing and forwarding infrastructure, which provides intercommunication between NATO organizations, Maritime Broadcast systems and National ACP127 networks.

Value Proposition: Military Message Handling Application Service offers the customers:

- The intercommunication between NATO and National Military Organizations,
- The automatic distribution of incoming and outgoing formal military messages based on information within a message and rules following the operational and administrative procedure,
- A workflow capability to support the coordination of message preparation.

Service Features: The Military Message Handling Application Service offers the customers the formal messaging capability with elements featuring:

- Access Management,
- Alternate Recipients,
- Conversation Prohibition,
- Deferred Delivery,
- Delivery Notification,
- Distribution List Expansion,
- Latest Delivery and Message Security Labelling
- Quality of Service adjustments based on different message priorities (e.g. expediting higher priority messages)

Service Flavours: The Military Message Handling Application service is available in multiple flavours based on the required functionality:

- **Standard**: Message reception only (through e-mail services).

Upon request (increased functionality):

- **Sending out**:
  - Desktop application need to be installed (AIMS)
  - Addressing needs to be available
  - Release authority to be established
  - SMAs and routing need to be configured. This flavour will be upon request. Note: multiple SMAs to be supported can be installed upon request
- **Serial ACP127 connections to National Gateways and Broadcast systems (with or without dual** homing).
- **Serial connections to end point locations including the installation of a PCTTY** (ACP127 protocol)
- **Complete AIFS system**.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Device Service
WPS004 – E-mail Services

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP030 - Tasker Tracker Enterprise Application Service

Service ID: APP030

Service Name: Tasker Tracker Enterprise Application Service

Portfolio Group: Application Services

Service Description: Tasker Tracker Enterprise Application Service provides the user with an Information Management capability for the tracking of Organisational tasks. The Tasker Tracker Enterprise Application Service offers a full workflow and collaboration tool which utilises the Microsoft SharePoint platform, providing the user with organisational tasking activities, namely; raising, delegating, monitoring and management of tasks.

Value Proposition: Tasker Tracker Enterprise Application Service offers the user a collaborative means for raising, delegating, executing, monitoring and management of organizational tasking activities. This delivers an efficient and auditable approach in support of all formal tasking activities; thus improving situational awareness and overall business operations.

Service Features: The Tasker Tracker Enterprise Application Service offers the user a highly configurable organizational tracking capability which supports the following core functionalities:

- Multi- user collaborative tasking,
- Integrated Document Management,
- Advanced Task Search Engine,
- Sub-Tasking,
- Traffic Light Monitoring System

The Tasker Tracker Application Service can be deployed interoperable with an existing Document Handling Application Service (APP031) or as an independent service.

Service Flavours: The service is available in a single flavour.

Available on:

NATO Secret
NATO Restricted
NATO Unclassified
Mission Secret
NATO Partner network (For NNHQ)

Service Prerequisites:

WPS001 – Managed Devices

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP031 - Enterprise Document Management Application Service

Service ID: APP031

Service Name: Enterprise Document Management Application Service

Portfolio Group: Application Services

Service Description: Enterprise Document Management Application Service provides the collaborative information management capability for Document Records Management. The Enterprise Document Management Application Service provides a collaborative environment for standardised document creation, management, storage and retrieval, integrated to the users' managed devices.

Value proposition: Enterprise Document Management Application Service offers the customers the support to easily access and maintain documented information by providing information access control, locating and retrieval of documentation and provisioning of storage.

Service Features: The Enterprise Document Management Application Service offers the user:

- Customizable organisational and data structures,
- Versioning,
- Check in/check out functionality,
- Search and browsing of documents,
- Alerting capability,
- Access options

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.0% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP032 - APMS Application Service

Service ID: APP032

Service Name: APMS Application Service

Portfolio Group: Application Services

Service Description: The APMS (Automated Personnel Management System) Application Service is a Human Resource tool, which provides users with the functionalities to support the management of personnel, jobs and organisations in the NATO static and deployed Command Structure. The APMS Application Service enables the user to access, collect, store, manage, analyse, present, process, and disseminate human resource information.

Value Proposition: The APMS Application Service offers the user improved accuracy, relevance and timelines of information, overall driving more efficient HR processes and procedures. Furthermore, day-today personnel management enables improvements for Manpower Modelling, Crisis Establishment (CE) and Crises Response Operations (CRO) by reducing analysis, reporting workloads and through the production of standardised executive summaries and reports.

Service Features: The APMS Application Service offers the user the functionality to provide:

- Personnel Management; In/Out Processing, Employee Self Service, Absence/Pass/Permits/Decorations Management
- Organisation Management; Manpower Modelling/Reporting, Skill-set/Job Description/Org Structure/CEtoPE Link Management
- Assignment; Assignment Posting, Job Hunter functionality
- Deployed Personnel Support Management; Accommodation/Arrivals/Departures/Passes/Permits Management
- Training Management; Training Course Management

Service Flavours: The service is available as a single flavour. Upon request, a customized version might be available.

Available on:

NATO Unclassified
NATO Secret
Resolute Support Mission Secret

Service Prerequisites:

WPS001 – Managed Device Servic

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP033 - INTEL FS Application Service

Service ID: APP033

Service Name: INTEL FS Application Service

Portfolio Group: Application Services

Service Description: The Intel FS (Intelligence Functional Service) Application Service provides an integrated, robust and flexible capability supporting a suite of services available throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to support the direction, collection, processing, and dissemination of intelligence in a timely and responsive manner in accordance with NATO policy, doctrine and guidance.

Value Proposition: Intel FS Application Service provides the NATO Intelligence Community with a capability that enables the following operational benefits:

- Sharing of intelligence services and data across NATO at all levels of command.
- Manage the direction, collection, processing, and dissemination of intelligence requirements.
- Enhance the dissemination of intelligence with Nations and other domains.
- Enhanced analysis and exploitation capabilities.
- Manage posting and publication of intelligence products.
- Information exchange supporting situational awareness, common operational picture and targeting.
- Support the management of the intelligence processes.
- Provide search and analytical capabilities to retrieve/analyse intelligence information.
- Support the generation and the management of Intelligence Information.
- Provide specialised functionalities in support of specific domains (imagery, local employee personnel, and battlespace objects).
- Provide intelligence collaboration and synchronisation mechanisms to share intelligence across NATO according to Communities of Interest.
- Support interoperability with external systems.
- Manage Users and Permissions.
- Support all operational mission types.

Service Features: The INTEL FS Application Service is comprised of the following features that combined support an overall intelligence cycle:

- Intelligence Direction (Request For Information (RFI) and Intelligence Requirement Management).
- Intelligence Search, and Analysis.
- Intelligence Processing – creation/management of intelligence products such as Battle Space Objects (BSO) and Intelligence Surveillance Reconnaissance products (ISR Products).
- Intelligence Management.
    - Maintenance of Intelligence products.
- Intelligence Dissemination.
    - Dissemination of intelligence products to the intended recipients.

Service Flavours: The INTEL FS Application Service can be fully customized and provided with different components enabled/disabled: LEP, RFI, Imagery, ASAS products, RSS, Administration, Domain Value management, CSD, etc.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 - Managed device service
APP055 - Core GIS Geospatial Services

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP034 - Integrated Engineering Management (IEMS) Application Service

Service ID: APP034

Service Name: Integrated Engineering Management (IEMS) Application Service

Portfolio Group: Application Services

Service Description: The Integrated Engineer Management System (IEMS) Application Service is an integrated asset management tool, which provides operation, support, maintenance and infrastructure management functionalities.

Value Proposition: The IEMS Application Service enables the user to support the maintenance of the SHAPE Infrastructure within accepted and agreed response times as per SHAPE' requirements. In addition, this application enables infrastructure project management, supports material management and SHAPE property disposal business processes.

Service Features: The IEMS Application Service offers a modular approach in support of the SHAPE Base Support Group within one single centralized database:

- Project Management
- Buildings Management
- Warehouse Management
- Budget Management
- Budget Long Range
- Reimbursable Customers Management
- Bunker Management
- Capital Items Management
- Non-expendable Items Management
- Utilities Consumption Management
- PWL Personnel Management
- Timekeeping Management
- Fire Brigade Management
- Proposal Disposal Office Management

Service Flavours: The IEMS Application Service is available as a single offering.

Available on:

NATO Unclassified
The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP035 - eLeave Application Service

Service ID: APP035

Service Name: eLeave Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The eLeave Application Service provides an organisation with an online environment, which allows it to effectively and easily manage and administer all Human Resources leave related activities in an automated and standardized manner.

Value Proposition: The eLeave application service provides a fully automated system, which supports the organization's HR leave processes. In doing so it delivers a standardized, accurate and paperless online environment in which employees, managers and Human Resources administrators can easily and efficiently manage leave activities; i.e. : "leave requests", "approval / rejection", "leave balances & statuses", …. As such it covers all the process steps; from leave submission to the eventual and final approval or rejection. The implementation of such a system greatly reduces the time and effort spent on the management and administration of all leave related activities and processes. Moreover, the e-leave IT system provides standardization across all HR leave activities. It should be noted, that it has been developed fully in line with NATO's HR processes, activities and business rules.

Service Features: The eLeave Application Service allows users, i.e. staff members, to request all types of leave (Annual Leave, Home Leave, Special Leave for Private Reasons, Special Leave on Marriage, Special Leave for Maternity and Paternity, Long Service Leave, Leave for Training, Leave for Military Service or Training and Unpaid Leave). The Service can also be used to report absence for health reasons (Sick Leave). In addition the service provides:

- Leave record for each staff member, including leave balances and home leave entitlements
- Automatic calculation of leave days (based on official holidays per duty location)
- Automatic e-mail notifications and tasks for approval
- Attachments (for sick leave certificates, etc.)
- Creation of calendar appointments from leave requests
- Personal detailed leave overviews for the staff members
- Reports for managers at various organizational levels
- Versioning of all leave data
- Archiving of previous years' requests
- Consideration of Annual leave cut-off dates in calculations
- Recording and parking of next year's leave to be processed by the end of the year

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure fir the Service is Per Database.

APP036 - FinS Application Service

Service ID: APP036

Service Name: FinS Application Service

Portfolio Group: Application Services

Service Description: The FinS Application Service provides the user with an Enterprise Resource Planning (ERP) system (based on the Oracle E-Business Suite Commercial Off-The-Shelf software and some extensions (iTravel)) with capabilities to perform streamlined budget execution, accounting, procurement, payments, and travel processes. It allows the customer to be compliant with NATO Financial Regulations (NFRs), Procurement Directives and International Public Sector Accounting Standards (IPSAS).

Value Proposition: The FinS Application Service offers the user greater transparency, flexibility, control and auditability over allocated and delegated budgets, thus facilitating NATO Strategic Commands, NATO Military Commands, NATO Agencies and other NATO Organizations focusing on their core business.

Service Features: The FinS Application Service provides the following functional features:

- General Ledger;
- Accounts Payable;
- Accounts Receivable;
- Cash Management;
- Fixed Assets;
- Purchasing;
- Advanced Procurement (iProcurement, Procurement Contacts, Service Procurement);
- Travel Management (Travel Requests and Travel Claims);

The FinS Application Service consists out of the following elements:

- FinS Operations: Daily management of hardware and software;
- FinS Incident and Problem Management;
- FinS Change Management: Change management in coordination with concerned stakeholders;
- FinS Training.

Service Flavours: The service is available as a single flavour, with available specific configurations.

Available on:

NATO Unclassified
NATO Restricted

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP037 - Performance Management Application Service

Service ID: APP037

Service Name: Performance Management Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The Performance Management Application provides a web-enabled platform which allows stakeholders to assess employee performance through goal-setting and tracking, customizable review forms and scales, 360 degree feedback gathered from peers, competency tracking, and more. The application supports the performance management processes and activities which ensure that goals are consistently met in and efficient and effective manner.

Value Proposition: The HR Performance Management service provides a strategic and integrated approach to increase the effectiveness of the organization by improving the performance of the people by developing the capabilities of teams and individual contributors. Furthermore this service enables:

- Greater transparency in the performance management process.
- Improved (regular) feedback for workforce.
- Encourages professional development.
- Get employees involved in their own progression.

Service Features: The Performance Management Service provides the following features:

- Ad Hoc Reviews
- Alerts / reminders
- Appraisal History Tracking
- Cascading Goals
- Competency Tracking
- Custom Rating Scales
- Goal Setting and Tracking
- Individual Development Plans
- Self Service Portal
- Performance appraisals
- Integrated reporting features (PDF, online)
- Support for review cycles (configurable)
- Notifications via email
- Performance Management Dashboard
- Reporting / Status reports

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Restricted

Service Prerequisites:

WPS001 – Managed Device Service

TBD – All staff, both civilian and military must be present in a core CCD HR database integrated with the HR Performance Management service.

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per User.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP038 - eRecruitment Application Service

Service ID: APP038

Service Name: eRecruitment Application Service

Portfolio Group: **Business** Application Services

Service Status: Pipeline

Service Description: The eRecruitment Application Service provides the customer with a modern, fully electronic capability to effectively and efficiently support recruitment campaign in line with NATO directives. This application supports the recruitment process from vacancy posting, video interviews, to successful candidate selection and onboarding for civilian personnel and various types of temporary workers at the NATO International Staff Centre, NATO International Military Staff, NCI Agency and NATO Alliance Ground Surveillance Management Agency.

Value Proposition: The eRecruitment Application Service drives a significant reduction in cost for the execution of a recruitment campaign and seriously improves operational efficiency and quality results through the use of the application. This is achieved through increased automation of tasks as it accelerates the recruitment campaign. The application offers automated workflows and a single point to access the web-based front end for the applicants and the specialized application frontend and backend for the hiring managers and hiring officials. The use of the application enables effective, efficient, quality, faster and less-costly management of recruitment campaigns. Through its introduction, the application eliminated the need to print and distribute a large number of documents for the various stakeholders involved in the recruitment process. As the capability is built on one single database instance, but with built-in data segregation for each NATO entity, it allows each organization to remain in control of its own recruitment campaigns but also for the HR officials to share data and knowledge about candidate application history as needed. Additionally this service, through its search and apply functionalities, offers the applicant a greater recruitment experience.

Furthermore, this application increases NATO's image and branding as an employer trough the presentation of vacancies to a larger number of NATO bodies onto the same online recruitment platform and in the improvement of results, through attracting a wider range of active and passive candidates.

Service Features: The eRecreuitment Application Service offers the user recruitment campaigns; online job-boards; collection and management of applications; asynchronous video interviews, recruitment screening and evaluation tools, together supporting candidate selection and store and share of application histories.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Recruitment Campaign**.**

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP039 - Enterprise Project Management (EPM) Application Service

Service ID: APP039

Service Name: Enterprise Project Management (EPM) Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The EPM Application Service provides the user with Project Management capabilities to support the creation and execution of related processes and activities. The EPM Application Service provides project start-up/planning/baselining/execution/control/collaboration, resource management, time accounting and reporting.

Value Proposition: The EPM Application Service enables the enforcement of common project management procedures, data centralization and improved accuracy and control to project progress, expenses, resource management, execution & control and reporting. Furthermore, projects utilizing the EPM Application Service benefit from easier redirection of resources to meet project demand and real-time monitoring of project performance.

Service Features:

- Project Execution and Control; Efficient execution of project controls towards effort and cost
- Time Accounting System; allows project staff resources to report project/non-project activities and time spent
- Reporting; Configurable reporting functionality
- Project Collaboration; based upon SharePoint technology enables store/share/act on projected related information (documents, issues, risks)

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Restricted

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per User.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP040 - Inventory/Asset Management Application Service

Service ID: APP040

Service Name: Inventory/Asset Management Application Service

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: The Inventory/Asset Management Application Service provides an ERP system based on Oracle E-Business Suite Commercial Off-The-Shelf Software, the capabilities of which are to collect, process, present and distribute consolidated information of assets, from a lifecycle perspective (acquisition to disposal). This service supports the centralized management of assets and is technically integrated within the centralized NATO Automated Financial System (CNAFS Application Service) to drive better visibility on reporting, decision-making, sustainable financial discipline, regulatory compliance (Inventory IPSAS 12), data integrity, optimized and efficient asset management processes. The Service provides the capabilities for operating Logistics in compliance with the Property Accounting Directives ACE 60-80 and the NCIA 'Under Construction Successor for the superseded NCSA OSI A-16-04.

Value proposition: The Inventory/Asset Management Application Service offers centrally managed Inventory and Order Management capabilities, with delegation of specific operational tasks to the local CSU's, integrated with already existing procurement and finance capabilities to drive efficiencies in the lifecycle of asset management. Furthermore, amongst other benefits, utilizing the Inventory/Asset Management Application Service facilitates easier redirection of asset resources as well as improving the operating costs by avoiding duplicated procurement and rationalizing inventory and assets including traceability.

Service Features: The Inventory/Asset Management Application Service offers the following features:

- Inventory Management (Warehouse Configuration Management, Asset Receiving, Creation and Labelling, Stock Availability Planning); Item management, asset movement, physical inventory and periodical cycle counting, inventory replenishment, reporting, quantity and value management.
- Order Management; customer account / CisPOC(MRAH) Assignment / custodian / shipping / delivery addresses management, internal/external.
- Asset Cost Accounting; asset valuation/weighted average cost (WAC) calculation, inventory accounting/reconciliation and auditing.
- Approval Hierarchy along with automatic notifications defined in the system also ensures control and visibility of Asset Procurement and movements.
- Auditing capabilities inherently present in the system can be used to fulfil internal/external checks and also for KPI's for any performance improvements.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per User.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP041 - Logistics Functional Area Services (LOGFAS) Application Service

Service ID: APP041

Service Name: Logistics Functional Area Services (LOGFAS) Application Service

Portfolio Group: Application Services

Service Description: The LOGFAS Application Service enables the user to collect, store, manage, analyse, present and distribute logistics information during NATO operational planning and execution.

Value Proposition: The standardization of logistics data and data formats and their timely exchange is the key to the success of complex logistics operations, especially to facilitate the coordination between the many deploying forces from multiple nations, with limited logistic assets and infrastructure capabilities. LOGFAS addresses the requirement to minimize the planning time for NATO deployments and to maximize the capability for rapid exchange of the associated plans, reports and other information. Furthermore, LOGFAS allows the user to query logistics information for specific item(s) across multiple units and nations.

Service Features: The LOGFAS Application Service is comprised of multiple modules, these are:

- ACROSS; Allied Commands Resource Optimization Software System comprises of the below sub-modules, all of which follow target oriented methodology and are used to calculate requirements on the battle decisive munitions to defeat targets conventional means, according to NATO level of ambition:
    - Air Defiance Munitions Expenditure Module (ADMEM)
    - Air to Ground Munitions Expenditure Module (AGMEM)
    - Land Forces Munitions Expenditure Module (LEMEM)
    - Maritime Munitions Expenditure Module (MARMEM)
- ADAMS/ADAMS Web; Allied Deployment and Movement Systems module supports strategic deployment and multinational deployment planning through provision of deployment plan development and feasibility testing.
- EVE/EVE Web; Effective Visible Execution provides monitoring of movement and transportation activities and provision for plan adjustments.
- CORSOM; Coalition Reception, Staging and Onward Movement provides visualization and oversight of theatre movements, during both deployment execution and sustainment operations.
- LOGREP; Logistics Reporting provides reporting capabilities that supports LOGUPDATE and LOGASSESSREP reports in pre-approved and standardized formats as laid out in NATO reporting directives.
- SPM/SDM; Sustainment Planning Module provides calculation functionality to support sustainment requirements for operations, packaging requirement for sustainment and strategic stockpile planning.
- GEOMAN; provides geographical information on the facilities, unit holdings and transportation networks.
- LDM; enables maintenance of information on force profiles and holdings, transportation assets, and planning data.

- LOGNET; LOGNET is the collaboration portal for the logistics community operating on bot NATO Unclassified and NATO Secret platforms.

Service Flavours:

LOGFAS: LOGFAS without ACROSS – releasable to NATO and PfP Nations[1];

LOGFAS+: LOGFAS including the ACROSS module – releasable only to NATO Nations;

Server based application: two types of clients (Windows or Windows + Web Client) and a PostgreSQL Database Server;

Standalone application: Windows application using local PostgreSQL Database

Collaboration web portal (LOGNET) on NS or on NU (accessible from the Internet).

Available on:

NATO Secret
Mission Secret
NATO Unclassified (LOGNET)

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[2] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] Release of NATO owned Software to Partner Nation is subject to NC3B approval.
[2] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP043 - Interactive Simulation Package (ISP) Application Service

Service ID: APP043

Service Name: Interactive Simulation Package (ISP) Application Service

Portfolio Group: Application Services

Service Description: The service provides a flexible, state-of-the-art solution to support the execution of air operations, which enables nations to simulate radar data in order to generate plot data to use it in a training and/or testing environment.

Value proposition: The service enables conduct of testing and exercises by providing necessary radar data.

Service Features: ISP enables generation of necessary data for execution of exercises for air operations, with particular focus at the NATO Integrated Air and Missile Defence System (NATINAMDS) community. More specifically, it enables:

- Modelling of airborne, sensor, and ECM exercise elements and to engineer scenarios by retrieval, positioning, manoeuvring, altering and manipulation of various elements via the graphical user interface;
- Performing of scenario management (retrieve, save, add, build, merge and delete);
- Performing of preview functions on the scenario;
- Execution and control of scenarios by starting, stopping, pausing, rewinding and forwarding the exercises;
- Activation and deactivation of radar sensors;
- Performing of interactive “real-time” changes, upon request, to alter the scenario during scenario execution;
- Providing of exercise support for flight plan printouts of selected missions and providing of the generation of flight plans, visible within the Multi AEGIS Site Emulator (MASE) system or any other system using the ADEXP flight plan message format for direct flight plan injection;
- Providing of realistic training for operational crews in the use of mechanical and electronic counter-measures (chaff simulation);
- Allow for the control of simulated fighter aircrafts using manoeuvrable targets

ISP is a standalone product, supported on Solaris, with the NISP configuration for the Solaris installation as preferred one. ISP provides input to the MASE system, but does not dependent on the MASE baseline version.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret

NATO Classified

Service Prerequisites:

Solaris operational system installed

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP045 - SIGINT COINS Application Service

Service ID: APP045

Service Name: SIGINT COINS Service

Portfolio Group: Application Services

Service Description: The Signals Intelligence (SIGINT) Support Service offers subject matter expertise for the Signals Intelligence Communications and Information System (COINS). SIGINT COINS is an integrated hard- and software capability for the dissemination, storage and processing of signal intelligence information to SACEUR, the NATO Commands, NACSI Nations and accredited partner Nations up to and including CTS/B level, which can be provided in a static HQ or cell or as a deployable kit.

SIGINT COINS Remote Support contains:

- 1st, 2nd and 3rd level user support – trouble shooting of hard- and software related problems.
- User support hotline – assistance for not hard- or software related problems.
- Liaison with other services – e.g. crypto management, EMSEC, CSSC (equipment repair/ exchange).
- Security accreditation support – assistance for accreditation and reaccreditation of sites.
- Assistance and support of mobile deployments of SIGINT COINS in operations (deployable kit)

Value Proposition: SIGINT COINS provides robust, secure communications between NATO Commands, NACSI nations and partner nations to allow improved exchange of vital, time sensitive special intelligence information and the applications to generate those products required by the Signals Intelligence Community. It is the only means for SACEUR to acquire special intelligence required for his mission. The service utilises the NATO SECRET LAN/ WAN and BICES as transfer medium for its encrypted data traffic. For this to achieve, it contains a collection of tools allowing the customer to share national content with NATO. The system provides portals for different information dissemination needs. The data in those portals can be easily searched with enterprise grade search tools to accommodate analyst requirements.

The service provides the maps and software required to display georaphical location information contained in reports on official NATO maps. It also provides a tool to generate, manipulate and display link diagrams supporting advanced link analysis.

Service Features:

- Assistance in the definition, development and implementation of new requirements.
- Provision of technical advice and expertise to NACSI nations, NACSI and NATO Commands directly or at meetings of relevant bodies and COI's.
- Information management support services – change management of information.
- Development and implementation of new hard- and software baselines whenever the trusted baseline requires changes.
- Change Control and Authorization support services - Chairing the SIGINT COINS Working Group; processing the CCP's and implementing the approved solutions resulting from the decisions of the WG.
- Exercise and operations support services – planning, provisioning, maintenance, user and logistics support of deployable SIGINT COINS kits.

- Documentation services – development of security related documentation and technical documentation and manuals.
- High Available Server Cluster and Storage system to ensure continuity of service.
- Security services – Authentication, certification, DLP and Malware protection Management, patch Management, event collection, security and system event monitoring.
- Data Management services – data storage, data maintenance (backup/ restore), data exchange and data import.
- Database services – SQL server based; maintenance and information management of specialized Databases.
- SharePoint services – Portals, document libraries, COI's, and other functions provided through SharePoint upon user request.
- Translation services – Tailored translation tool trusted by NACSI Nations and NATO.
- Email and messaging services – MS Exchange and MS Lync based linked to SharePoint.
- Planning services - SIGINT COINS configuration management in support of changes at the site or establishing a new site.
- License management services.
- Information gateway service – provisioning of secure transfer of information between NATO SECRET and SIGINT COINS (Data Diode System Service)

New Service Request:

A request and an approval of the inclusion of a new site in the Operational Validation Letter issued by ACOS SHAPE J2 is required prior to completion of the Customer Request Form.

Service Flavours: TBD

Available on:

SIGINT COINS is a cryptographically isolated network.

Service Prerequisites:

- SHAPE J2 declaration of Operational Validation of the installation
- NCGS (NS-WAN) or BICES connectivity.
- Crypto Management and Distribution services.
- CTS Registry services.

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP046 - HMART Application Service

Service ID: APP046

Service Name: HMART Application Service

Portfolio Group: Application Services

Service Description: The Human Intelligence (HUMINT) and Counter Intelligence (CI) support service offers subject matter expertise (SME) support to the applications used by HUMINT and CI. The applications facilitate users to collect intelligence provided by human sources. It includes the systematic and controlled collection and exploitation of HUMINT/CI by interaction with human sources, objects, or individuals. HUMINT and CI activities involve safeguarding and exploitation of human sources, and efficient collection, reporting and analysis integrated within the overall intelligence environment to provide decision makers with timely and accurate information necessary for conducting successful military operations.

Value Proposition: The combination of the two HMART modules (HMART SD and HMART OM) provides support to the HUMINT process for NATO lead operations ranging from:

- Securely managing the highly sensitive identities of human sources,
- Support to HUMINT mission planning.
- NATO HUMINT doctrine standards based report writing (AIntP-5).
- Workflow driven life cycles of reports providing the mechanism to improve the quality of reporting and ensure the proper sanitization of information.

Service Features: HMART consists of two modules that serve different parts of HUMINT and CI operations.

HMART SD (Source management and de-confliction) – a stand-alone module running on secured and ruggedized laptops within NATO lead operations. The purpose of the module is to maintain information that could potentially reveal the identity of the source. The module has the following functionalities:

- Management of a dossiers of human sources
- De-confliction of human sources based on biographic and biometric characteristics.
    - Biometric comparison based on biometric modalities of face and finger print information.
    - Biographic (or heuristic) characteristics that are the basis for de-confliction other than biometrics. Eye colour, estimated year of birth, living location, weight, tribe and many other fields considered to identify possible duplicate sources.
- Secured exchange of source information within the J2X command structure.
- Powerful search functions to allow for analytical processing of source information. Structured searches based on metadata fields, geographically oriented search and unstructured full text search in order to quickly identify the human source coverage within an area of operation.

HMART OM (Online Module) – an online reporting module for HUMINT operations and support to HUMINT mission planning.

- Internal and external report writing based on NATO HUMINT doctrine (AIntP-5)
    - Fragmentation Order (FRAGO)
    - Debriefing Area Reconnaissance (DBA RECCE)

- Contact Form
- HUMINT Report
- CI Report (CI)
- Liaison Contact Report (CI)

- A workflow driven report life cycle that contributes to timely reporting and improved quality of reports produced.
- An operations (OPS) matrix used for HUMINT mission de-confliction at J2X level.
- Support to analytical processes. E.g. identify the operational value of a source based on information provided by a source.
- Interoperability with J2 for external reports (CI Report and HUMINT Report)
- A central repository for all HUMINT reporting containing historical reference data and supports data analysis.

Sub-Services:

- HMART implementation, integration and customization.
- Operations and maintenance (HW and SW upgrade, annual biometric maintenance licences, release and change management, system administration, monitoring, etc.).
- Training of HMART users and administrators either at the NCI Agency, HUMINT Centre of Excellence (HCOE) or on-site.
- HMART support during the preparation and conduct of operations, exercises and experiments.
- Information gathering for technical and training support.

This service provides full or partial technical and training support in the HUMINT information gathering, process and design, and production of tailor made reports.

Service Flavours: HMART supports HUMINT/CI operations by two distinct operational modules.

HMART SD – deployed on stand-alone laptops to provide the best protection of the identities of human sources.
HMART OM – as a networked capability used within the J2X structure for reporting and support to HUMINT/CI mission planning.

Available on:

NATO Unclassified (Training and exercise only)
NATO Secret (HMART OM)
NATO Secret stand-alone (HMART SD)

Service Prerequisites:

HMART SD

HMART SD is designed to run on stand-alone ruggedized laptops (TEMPEST level B) with hardware encrypted HDD when used for operational purposes.

HMART OM

HMART SD is a fully web based application that requires a server installation. Client machines only require a HTML5 compatible browser like Chrome or IE9 or later.

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP047 - Allied Command Operations Open Source System (AOSS) Application Service

Service ID: APP047

Service Name: Allied Command Operations Open Source System (AOSS)

Portfolio Group: Application Services

Service Description: AOSS is a centralized web-based application that constantly collects open and subscribed source information from news agencies and Internet and transfers it in real time to the different networks within NATO. The core of AOSS uses the enormously powerful IDOL search engine from Hewlett-Packard, which allows AOSS to index a nearly unlimited amount of any type of documents and search them rapidly. Being a semantic engine, it offers “entity extraction” (i.e. it recognises persons, places, amounts, etc.) as well as multilingual automatic categorisation, highlighting, taxonomies, metadata extraction, clustering and a lot more.

Value Proposition: An estimated 80% of required information available for use in open sources for specific information vital for a deep analysis is available in newspapers, magazines, industry newsletters, television transcripts, and blogs. By using OSINT services, the Intel Analysts are able to get pertinent and essential information in the most effective way. Intel Analysts will find in AOSS the Political, Economic and Military Indicators and Trends they need to correlate with their findings, and updates on the classified side. Public Information Officers will use the watcher and report generation features to produce a daily Open Source compilation for their Commander-in-Chief. OSINT is unclassified and available, but link-crawling search engines like Google do not always access it. By researching various sources online, the OSINT service provides more information about what a company, individual, group, or country is up to, but it’s not always easily found. The use of OSINT has grown within the private sector as well as being a mainstay of the military and the intelligence services for years.

- **Uncovering**: Knowing who knows about the data and knowing where to look and we get the appropriate data are the key process which leverages distributed centres of expertise and archival knowledge.
- **Discrimination**: Careful discrimination between good and bad sources, current and outdated sources and relevant and irrelevant sources is part of the unique value of the process.
- **Refining**: *The most important value added* by the process is that of Refining; the final research report may be as short as a paragraph or a page.
- **Delivery**: The best intelligence/research in the world is useless if it cannot be delivered to the client in a timely fashion and in a format that can be easily understood.

Service Features: The AOSS Service offers the user:

- Real-time (24/7) indexation of feeds and images from external agencies (e.g. Reuters, Associated Press, Factiva (Dow Jones), Agence France Press, etc.) to make them available on the NATO networks.
- News feeds categorization by topics of interest.
- Web services for integration into other systems
- A simple and advanced search through the feeds and images.
- Watcher service: automatic search queries with notifications of new hints (also on mobile devices).
- Geocoding: the search results per each country visualised on the World Map.

- A cluster map tool to identify areas of high activities displaying data using a heat image.
- Statistics, trends and analysis of news feeds.
- Alerting: COI related content Email dispatching.
- A scrapbook metaphor to generate draft Intel products and briefs.

Service Flavours: The AOSS is available with different resources, and the following components are available separately:

- GeoTagger: produces GIS layers (KML and NVG 1.4 and 1.5)
- RSS feed provisioning (e.g. into SharePoint)
- Topic based Email notification service
- A set of web services that can be used without the AOSS front-end interface
    - Text highlighting web service
    - Category suggestion (meta tagging)
- Document Processing Service (DPS) powerful event based file handling service

Available on:

Internet facing
NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

WPS001 - Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP048 - Analyst Notebook (ANB) Application Service

Service ID: APP048

Service Name: Analyst Notebook (ANB) Application Service

Portfolio Group: Application Services

Service Description: ANB offers a visual analysis environment designed to help analysts to turn large sets of disparate information into high-quality actionable intelligence and to help identify, predict, and prevent criminal, terrorist, and fraudulent activities. A flexible data acquisition approach allows analysts to more quickly collate both structured and unstructured information to help build a single, cohesive intelligence picture. The flexible data model and visualization environment coupled with a wide range of visual analysis tools help users build multiple views for detailed network, temporal, statistical, or geospatial analysis and reduce the time taken to identify key connections, networks, patterns and trends that may exist. The results gained from this detailed analysis may be shared via intuitive and visual briefing charts or visualizations that can be included in end intelligence products.

Value Proposition:

- Flexible data acquisition: rapidly import structured data, simplify the manual data entry process, connect to and query available data sources.
- Flexible data model and representation (environment that offers users flexibility in how data is modelled and visualized).
- Simple communication of complex data (intuitive and easy-to-follow visual briefing charts).
- Powerful analysis capabilities (wide range of analysis capabilities).
- Extensibility (see *Service Flavours)*.

Service Features: The Analyst Notebook (ANB) Service offers the user:

- Acquire data from disparate sources in order to piece together a coordinated picture that allows for an effective, more accurate analysis of available information.
- Establish key “who, what, where, when and why” information by analysing and visualizing data in multiple ways including association, temporal, geospatial, statistical, spreadsheet views and social network analysis, "list most connected" and "find connected networks".
- Identify connections, patterns, trends and key intelligence within a wide range of data types that might otherwise be missed.
- Discover duplicate information within data by leveraging intelligent semantic smart matching capabilities.
- Increase understanding of structure, hierarchy, method of operations and key individuals or groups within criminal, fraudulent and terrorist networks and the roles they may play, helping to guide future operational planning and resource allocation.
- Create clear and concise briefing charts to simplify complex data in support of more timely and accurate operational decision making.
- Simplify the communication of complex data to enable timely and accurate operational decision making.
- Capitalize on rapid deployment that delivers productivity gains quickly using a well-established visual analysis solution.

Service Flavours: The service is available as a single flavour. However, there is an extensive range of options available to extend further i2 Analyst's Notebook capabilities in order to provide even greater value to analysts and their wider organization. These come with additional costs:

- **Data Centric Analysis**—IBM i2 Analyst's Notebook Premium
- **Data Acquisition**—IBM i2 iBridge, IBM i2 Information Exchange for Analysis Search
- **Geospatial Analysis**—IBM i2 Analyst's Notebook Connector for ESRI
- **Unstructured Data Analysis**—IBM i2 Text Chart, IBM i2 Text Chart Auto Mark
- **Collaboration**—IBM i2 Analyze (via i2 Analyst's Notebook Premium), IBM i2 iBase
- **Extensibility**—IBM i2 Analyst's Notebook SDK

Available on:

NATO Unclassified
NATO Secret
Mission Secret (MS)

Service Prerequisites:

WPS001 - Managed device service.

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP049 - Integrated Command and Control (ICC) Application Service

Service ID: APP049

Service Name: Integrated Command and Control (ICC) Application Service

Portfolio Group: Application Service

Service Description: The NATO-wide Integrated Command and Control Software for Air Operations (ICC) is an integrated Command, Control, Communications and Intelligence/Information (C3I2) system that provides information management and decision support to NATO air operation activities during peacetime, exercise and crises. Currently, ICC provides functional support for the most critical Air C2 functions at the Joint Force Command, Air Command, and Combined Air Operations Centre levels. ICC consists of client and server applications, which run on Commercial-off-the-shelf (COTS) platforms. It uses an Oracle relational database management system with presenting via state-of-the-art Java-based graphical user interface (GUI).

Value proposition: ICC provides capabilities for integrated planning, tasking, operations, information management and decision support to operational and tactical level Air operations during peacetime, exercise, crisis and conflict. ICC also provides functional support for the most critical Air Command and Control (Air C2) functions at Air Component Command (ACC/JFACC) and Combined Air Operations Centre (CAOC) levels.

Service Features:

- Generation of Air Operations Directives (AOD)
- Generation of Airspace Control Orders (ACO)
- Generation of Air Tasking Orders (ATO)
- A capability for executing current operations at ACC/JFAC and CAOC units
- Automated status reporting
- Display of a Joint Common Operational Picture (COP) including the Recognized Air Picture (RAP) as provided from the Networked Interoperable (near) Real-time Information Services (NIRIS)
- Display of Shared Early Warning (SEW) information.
- TMD situational awareness and missile engagement (LSID)
- Replication of ICC related C2 data between sites
- Web-services interface to provide Air C2 information to interfacing systems

Service Flavours:

ICC fully integrated capability – Includes the ICC software, documentation, platform and database binaries for building a full ICC system with the full set of functionality provided by the ICC server and client.

ICC software – Includes all ICC software components and documentation to build either a full ICC site (server and clients) or ICC client workstations who can operate stand-alone (e.g. for parsing ATOs) and which would be able to remotely connect to a full ICC site.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Devices

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP050 - Air Command and Control Systems (ACCS) Application Service

Service ID: APP050

Service Name: Air Command and Control Systems (ACCS) Application Service

Portfolio Group: Application Service

Service Description: Air Command and Control System (ACCS) as a service provides Air Command and Control services through a modern and integrated system being deployed at various user sites. It enables seamless Air C2 operations to operate across multiple ACCS locations.

The Air Command and Control System (ACCS) First Level of Operational Capability (LOC1) – the current running version of ACCS - is deployed in commonly and nationally funded entities. The commonly funded entities are the Combined Air Operations Centre (CAOC) and the Air Control Centre/RAP Production Centre/Sensor Fusion Post (ARS). A CAOC or an ARS may be static or Deployable (DCAOC and DARS). The combined implementation of a CAOC and an ARS constitutes a CARS (Combined ARS).

Value Proposition: The value of ACCS is the integration of almost all relevant functions and external interfaces required for executing seamless Air C2 Operations within a network of ACCS sites at different level. Those functions can be installed at static sites as well as implemented as deployable or mobile site configurations.

Service Features:

OPS Level	Services
(D)ARS	The (deployable) ARS is a combination of the individual ACCS entities ACC, RPC and SFP. The Air Control Centre (ACC) is the entity in charge of air mission control to manage both the main defence forces within the design area and a proportion of the rapid reaction force. The ACC: • Is the real-time (RT) battle management entity; • Performs air mission control for all types of manned air missions and SAM weapons within a designed area; • Provides SAM weapon preparation; • Provides ATC services. The RAP Production Centre (RPC) is an air surveillance entity which produces and disseminates the RAP data within its assigned AOR, it: • Receives land and maritime surface tracks and sub-surface tracks from external links and disseminates them to the ACCS users. • Manages its subordinate and allocated ACCS surveillance areas in accordance with orders and priorities received from the CAOC. The Sensor Fusion Post (SFP) is an air-surveillance entity, which is in charge of the receipt of data from various sensor sources, both from within or outside the ACCS programme, in order to provide the basis for establishment and the maintenance of an RAP. The SFP:

	• Develops a local air picture (LAP) through the fusion of data from both active and passive sensors; • Reports on the status and performance of subordinate sensors; • Controls the sensor detection and responds to anti-radiation missile (ARM) threat and electronic counter-measures (ECM) activity.
(D)CAOC	The (deployable) CAOC is the entity in charge of the tasking of the assigned air assets, it: • Plans and conducts the tasking of air operations and C^2 resources configuration within a designed Area of Responsibility (AOR); • Supervises and monitors execution of tasking and analyses the results; Coordinates with land, maritime and national forces as well as with other NATO and National agencies.

Service Prerequisites: ACCS requires as dedicated operating platform consisting of CIS hardware, communications, COTS Software ACCS functional software and ACCS operational data. External system and inter-site interfaces require to be protected through firewalls as well as boundary protection services.

Service Flavours: ACCS consists of several standardized entity types which are used in different combinations to build ACCS operational sites at different level of operational commands:

- (D)ARS at tactical level,
- (D)CAOC at tactical and strategic level and
- CARS as a combination of a ARS collocated with a CAOC at the same location.

Available on:

NATO Secret

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics

- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP051 - NATO Integrated Solaris Platform (NISP) Service

Service ID: APP051

Service Name: NATO Integrated Solaris Platform (NISP) Service

Portfolio Group: Infrastructure Service

Service Description: The NATO Integrated Solaris Platform (NISP) has been developed as a tool to work alongside the Oracle Solaris operating system (OS), simplifying the Solaris installation and common system administration tasks. NISP provides the means for implementing a networked platform, open to a range of applications, which ensures site installations are easier to maintain and can be supported centrally. NISP has become the standardised general purpose system configuration tool, suitable for all AirC2 applications supported by the NCI Agency.

Value proposition: NISP realizes the value at the user side by standardizing the Solaris based Operating System platform installation and configuration while securing the installation in accordance with NCIRC mandated security settings.

Service Features: The NISP Service offers the user:

- Simplified installation and maintenance of Oracle Solaris based Operating System Platform,
- Easing the tasks of the system administrator by providing a rich set of scripts for installation and administration,
- Securing this OS platform by applying a pre-configured set-up as required for NATO networks,
- Providing security and OS patches either periodically or on request by the user,
- Standardized the Oracle Solaris based platforms for easing system platform support and troubleshooting,
- Comprehensive documentation for system installation, configuration and administration,
- Supports SPARC as well as Intel x86 based hardware.

Service Flavours: NISP flavours that the customers can choose from are:

- NISP 3.6.x for systems based on Solaris 10,
- NISP 4.x.x for systems based on Solaris 11.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites: NISP requires a license for the Oracle Solaris operating system IAW Oracle license terms and conditions.

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning

- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP052 - Application Layer Firewall for Link 1 Application Service

Service ID: APP052

Service Name: Application Layer Firewall for Link 1 Application Service (Formerly known as Air Situation Data Exchange (ASDE))

Portfolio Group: Application Service

Service Description: The purpose of the Application Layer Firewall for Link 1 service is to:

- Allow the controlled exchange of unclassified Link 1 data with partner nations;
- Protect the Link 1 interface of NATO CRC's from external Link 1 connections;
- Provide a solution of exchanging Link 1 data across systems of different NATO classification without filtering data.

Value Proposition: The Application Layer Firewall for Link 1 acts as a border protection device for NATO Link 1 connections. The NATO requirement for a bi-directional exchange of a RAP between NATO nations and PN resulted in the development of the Application Layer Firewall for Link 1. This system manages the controlled exchange of air picture data by filtering and downgrading the classification of the NATO air picture in such a manner that it is releasable to partner nations. The basis for the data exchange through the Application Layer Firewall for Link 1 system is the Tactical Data Link (TDL) Link 1. The system has since been extended to allow for the full exchange of Link 1 data between systems of different NATO classifications.

Service Features: The Application Layer Firewall for Link 1 supports the following features:

Filtering Mode: Allows the exchange of RAP with a NATO Partner nation by declassifying the Link 1 messages to a level of NATO Unclassified. In filtering mode, the Application Layer Firewall for Link 1 system will allow four operational modes:

- Peacetime Operations Mode
- Exercise Operations Mode
- Crisis Response Operations Mode
- Article 5 Operations Mode

The operational modes will determine the set of filter rules the Application Layer Firewall for Link 1 Buffer and LFF will apply.
The Application Layer Firewall for Link 1 security enhancing capability provides the following capabilities by implementing the security requirements:

- Coordinate conversion: masking of the originator site positions by using an arbitrary, bi-laterally agreed Data Link Reference Point (DLRP);
- Geographic filtering: selection of information for data exchange based on geographical areas;
- Data/Message filtering: message and data field filtering for sensitive information;
- Validation: message frame validation (on receipt from PN only).
- The Application Layer Firewall for Link 1 security enforcing capability provides the following capability;
- Trusted computing base: verification of message fields filtering and message frame validation.

Symmetrical Mode: Allows the exchange of unfiltered RAP within NATO by protecting the interface to ensure that only Link 1 messages are exchanged on the interface.

Supported configuration and Interface Standards:

The Application Layer Firewall for Link 1 supports both filtering mode and symmetrical mode. Regardless of the mode, the software and hardware requirements are identical and no change of hardware / software is required to alter the mode of operation. The mode of operation is in fact a configuration parameter to be controlled by the system administrator. The Application Layer Firewall for Link 1 implements the Tactical Data Link protocol Link 1 in accordance with STANAG 5501, edition 6.

The service currently installed is Application Layer Firewall for Link 1 version 4.0.1 and all sites are currently running this baseline. This is a NATO Baseline under the governance and Configuration Control of the AirC2 SC.

The Application Layer Firewall for Link 1 is supported by:

3- Provision of Application Layer Firewall for Link 1 Software
4- Helpdesk and provision of level 1 to 3 support through the Helpdesk
5- On-site interventions for installation and/or trouble shooting
6- Engineering/application support covering
   a. Product and Configuration Management
   b. Product baseline updates
   c. Application Layer Firewall for Link 1 Product Accreditation

Service Flavours: Typically, the NCI Agency supports two fielded versions, the recent and the previous releases installed in the field.

Available on: The Application Layer Firewall for Link 1 (NATO Side) supports any security classification as required by the data handled reaching from NC to NS. The Application Layer Firewall for Link 1 (Partner Side) supports any security classification as required by the data handled reaching from NU to NC. The Application Layer Firewall for Link 1 software itself is classified as NR and the system is delivered as an NR system with software pre-installed.

Service Prerequisites:

APP051 - NISP Service

In addition to the service prerequisites, the hardware, software and connection requirements are:

- Existing serial Link 1 connections must be available
- Approved Application Layer Firewall for Link 1 Server (Currently this is restricted to Oracle 5120 or Fujitsu M10 Server)
- MPS-1000 Serial interface server.
- Communication lines, network infrastructure

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation

- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP053 - Multi Airborne Early Warning Ground Integration Segment Site Emulator (MASE) Application Service

Service ID: APP053

Service Name: Multi Airborne Early Warning Ground Integration Segment (AEGIS) Site Emulator (MASE) Application Service

Portfolio Group: Application Service

Service Description: The MASE Application Service provides a NCI Agency product and support of it, with the following purpose:

- Production of a real-time recognized air picture (RAP);
- Identification and exchange of the RAP with other military or civilian entities;
- Battlespace management and provision of weapons guidance solutions;
- Flight Plan processing and real-time interface to feeds supplied by ATC centres.

Value Proposition: MASE is a flexible, state-of-the-art solution to support the execution of air operations. Both military and civilian radars can be connected using a large variety of interface protocols on dedicated lines or packet switched networks. The sensor data from these sources is processed using a multi radar tracker, which produces the real-time air picture which can then be forwarded to other military installations. Flight plan data from civilian or military Air Traffic Control (ATC) centres are received, correlated with the real-time air picture and displayed to the operational user to support identification of aircraft. The Battlespace Management function assists the operational users in threat assessment and allocation of weapon resources. With the optional addition of the CRC System Interface (CSI), command and control can be performed on datalinks including Link 11(A&B) and Link 16. Threats can be engaged with either fighters or surface-to-air missile (SAM) units. When engaging with fighters, the assigned intercept controller can select between various types of guidance solutions depending on the fighters' capabilities and the prevailing tactical situation.

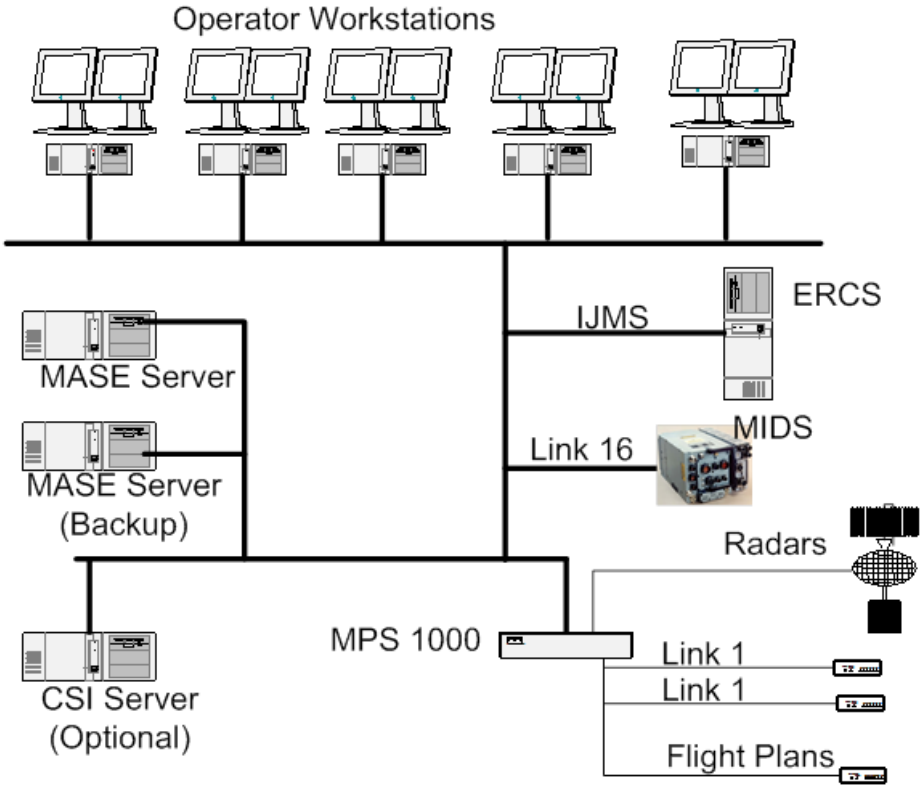
Service Features:

Sensor Integration – Allows to connect any number of radars to produce a locally generated Air Picture. Radar interfaces include but are not limited to : ASTERIX, JASR8, RMP, DDL, HADR, CD2, RSRP, T101, Cardion, T92, (A)S29, S743D, SRT, RAT31DL. The RAP produced is correlated into the Common Operating Picture (COP) and forwarded to connected units using the Link 1 interface.

Command and Control – Though the flight plan interface, tracks created from the RAP Production can automatically be identified. The Identification is managed with neighboring CRC's using the standard Link 1 messages for maintaining consistency across different military locations. The Weapons Allocator functionality allows for interceptor guidance and pairing to be performed. In addition, with the CRC System Interface (CSI) extension, Command and Control can be performed across the Link 11A/B and Link 16 datalinks. Enabling the operator to manage not only fighters but also land and naval units.

User Interface – The MASE User Interface has been completely re-designed, implemented upon a modern GUI engine and made more maintainable through the use of Java development. In the future, the legacy console will be completely replaced by the new MASE Integrated Console Environment (MICE). MICE has been developed together with the NPC CSI Section to ensure that future HMI updates can be achieved in a quicker, more cost effective manner.

Below figure outlines MASE in a typical use case:



Supported configuration – MASE encompasses client server architecture, with dedicated server applications for the main tasks as real-time air picture establishment and interfacing external systems, interconnecting dedicated MASE operator workstations for the operational display through a standard UDP/IP network. The serial interfaces (for both radars and flight plans) are brought into the MASE system through the MPS-1000 serial interface device.

Supported Interface Standards – JASR8, RMP, DDL, (A)S29, RAT31DL, HADR, ASTERIX, CD2, RSRP, S743D, T101, Cardion, T92, SRT. Through the CSI, the following interface standards are supported: Link 16 Link 11A, Link 11B, ATDL-1, Link 22, FFI, VMF, OTHT-Gold.

Supported data link interfaces – Link 1 in accordance with STANAG 5501, IJMS .

Hardware- Software and CIS requirements:

- NCI Agency (NPC) Integrated Solaris platform (NISP) as a secured Solaris OS platform;
- X86 or SPARC based server HW able to run NISP/Solaris;
- MPS-1000 Serial interface server;
- Communication lines, network infrastructure.

MASE is supported by:

- Provision of MASE Software
- Helpdesk and provision of level 1 to 3 support through the Helpdesk
- On-site interventions for installation and/or trouble shooting
- Engineering/application support covering:
  - Product and Configuration Management;

- Product baseline updates;
- Safety assessment supporting a customer side SIL 1 claim.

Service Prerequisites:

WPS001 – Managed Devices

Additional requirements:

- Existing serial Link 1 connections must be available
- Existing radar interfaces must be available
- If required, flight plan interfaces should also be available.

Service Flavours: Typically, the NCI Agency supports two fielded versions, the recent and the previous releases installed in the field. NATO Baseline is under the governance and Configuration Control of the AirC2 SC.

Available on: MASE supports any security classification from NC to NS.

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP054 - L16@29k Application Service

Service ID: APP054

Service Name: L16@29k Application Service

Portfolio Group: Application Service

Service Description: The Link 16@29K system allows a Cost system to connect to a MIDS terminal and it:

- Allows the exchange of Link 16 (Platform D) data with other units on the same Link 16 network.
- Allows the MIDS terminal to be remotely controlled (On / Off Standby);
- Monitors the system discretes of the Link 16 Ground Equipment Suite.

Value Proposition: L16@29K allows the exchange of encrypted Link 16 data with other units on the same Link 16 RF Network. When connected through IP based crypto's the L16@29K allows for remote MIDS to be connected to a central C2 system

Service Features: L16@29K supports the following features:

- Local Mode : The L16@29K system is directly connected to the C2 host system using a MIDS Platform D interface. The MIDS is connected directly to an antenna at the physical location of the C2 host system.
- Remote Mode : The L16@29K system is situated in a remote location (due to UHF Coverage limitations). The system shares a platform D interface with the host system across an encrypted TCP IP connection. The MIDS is connected directly to an antenna at the remote location and is controlled remotely from the C2 host system.

Supported Interface Standards: The L16@29K system implements the Tactical Data Link protocol Link 16 in accordance with STANAG 5516, edition 2. The Platform D interface is currently supporting Block Cycle release 2.

Service Flavours: The Service is available as a single flavour. In the future, NCI Agency will provide software updates in order to maintain/develop the current baseline.

Available on:

NATO Secret

Service Prerequisites:

None

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management

- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP055 - Core Geographic Information System (GIS) Application Service

Service ID: APP055

Service Name: Core Geographic Information System (GIS) Application Service

Portfolio Group: Application Services

Service Description: The Core Geographic Information System (GIS) Application Service is composed of subservices, which serve multiple purposes. The service is primarily based on the commercial off-the shelf ESRI software provides other Functional Services with a common set of geospatial information (Geospatial Service) to ensure that 'everyone is operating off the same map', thereby eliminating the need for other FSs to develop their own mapping solutions and maintaining their own set of geospatial information. In addition, the Core GIS enables anyone in the NATO Command Structure (NCS) to see available geospatial information like maps or imagery. Core GIS provides base maps/foundation Geospatial Information (GI)/geo location reference to all users and systems. The Core GIS also contains a functional area system (Geography Service) for dedicated geo professionals to enable the Core GIS Geospatial Services to be managed and administered. The Geography Services is implemented at each NCS site with high-end workstations and displays, large format plotting, and scanning infrastructure.

Value Proposition: The Core GIS Application Service provides customers with a suite of data, services and products that ensure all phases of military operations are conducted on the same spatial reference. Furthermore, it provides the Accredited/Single Geospatial Information Service Provision (authoritative repository for Geospatial Information).

Service Features: The current Core GIS Application Service consists of:

> **Cartographic Workshop**, which allows Geo-Technicians to create and maintain the Digital Geographic Information baselines, generate products, and publish and maintain geospatial services via the NATO Core GIS Server. The Cartographic Workshop comprises several high-end workstations for geo processing, and other peripherals such as an A0 plotter, A0 scanner, office printer, DVD production station, and infrastructure equipment
> **The Core GIS Server**, which is used to provide geographic products such as electronic maps or other geospatial information in digital form to Functional Services and FASs using international standards such as Web Map Service (WMS), Web Feature Service (WFS), Web Coverage Service (WCS), Web Processing Services (WP).

Service Flavours: The service is available as a single flavour.

Available on: NATO Bi-SC Core GIS service is available on the NS, MS, KFOR and RSM network. However, the service may be available on the customer's choice of security domain, as well. In case of national security domain, the customer is responsible for the accreditation and license module.

Service Prerequisites:

> WPS001 - Managed device service.
> Client: Windows 7 or Higher
> Server: Windows 2012 R2 or Higher.
> Detailed HW/SW requirements available upon request

Standard Service Support Levels:

Service Availability[1] Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP056 - ISR Collection Management Tool (ICMT) Application Service

Service ID: APP056

Service Name: ISR Collection Management Tool (ICMT)

Portfolio Group: Application Services

Service Description: The ICMT Service provides a capability to effectively manage the satisfaction of Prioritized Intelligence Requirements (PIRs): plan, task, monitor theatre-wide ISR collection capabilities, manage intelligence documents, and disseminate products. It also facilitates the collection of short-notice requests and requirements in a timely manner. The ICMT Tool has two functions: Intelligence Requirements Management function (IRM) and Collection Management function (CM), of which IRM usually is not used by the NATO entities. Collection Management function supports users in developing and disseminating CRs. The purpose of CRs is to combine (or bundle) similar Essential Elements of Information (EEIs) from the ICP (similar with regards to locations, time and required ISR capabilities) to propose doing as much as possible with the limited ISR resources. CRs are recorded and tracked in the ISR Plan with associations to the EEIs that they satisfy in the ICP. The system provides support to process Collection Requirements List (CRL) and Collection Task List (CTL). When collection coordination is required CRs are passed up the chain of command as validated and prioritised CRs in the CRL. At the joint level CRs assigned to subordinate commands/units are disseminated as CTL. ICMT provides support to develop and disseminate Collection & Exploitation Plan (CXP). The CXP is the plan that provides detail of the tasks assigned to specific ISR capabilities to meet the formation's collection requirements. The CXP is based upon own formation's or CRs assigned from the JCMB received through the CTL. ICMT also provides functionality to disseminate CRs as ISR Requests and Tasks (ISRRs), and to manage received ISRRs.

Value Proposition: ICMT is a client/server solution making it possible for the different roles involved in the IRM & CM processes to work in parallel on a common database. Support for development of Intelligence Requirements and Intelligence Collection Plan (ICP) is provided in the new Intel Collection Plan workspace. Support for the management of Requests for Information (RFI) is improved and now supported in the new Requests workspace. Additional values are:

- Support for dissemination of the ICP in xml format.
- Support for development of both Collection Requirements (CR) and ISR Plans are new capabilities provided in the ISR Plan workspace.
- New capabilities to manage ISR Requests (ISRREQ) and ISR Tasks, which is a significant improvement of support for Collection Management. Collection Requirements can easily be exchanged between commands and ISR units as ISR Requests and ISR Tasks.
- Dissemination of the Collection Task List (CTL) in xml format is supported.
- Support to import of and export to excel sheets that comply with MAJIIC 2 Bravo .1 Baseline for the information content.
- Configurable to connect to the MAJIIC 2 Bravo .1 JISR COI Technical Services enabling interoperability with national and NATO systems that are Bravo.1 compliant.

Service Features:

- Intelligence Requirement Management
    - Develop, receive, manage and track Priority Intelligence Requirements (PIRs) and

IRs.
    - Developing and maintaining the ICP.
- Collection Management
    - Develop and disseminate CRs (CRLs and CTLs)
    - Process Collection Requirements List (CRL)
    - Process Collection Task List (CTL)
    - Develop and disseminate Collection & Exploitation Plan (CXP)
    - Functionality to disseminate CRs as ISR Requests and ISR Tasks (ISRRs)
    - Manage received ISRRs.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 – Managed Device Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability
Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP057 - INTEL FS SIGINT Capability (ISC) Application Service

Service ID: APP057

Service Name: INTEL FS SIGINT Capability (ISC) Application Service

Portfolio Group: Application Services

Service Description: The INTEL FS SIGINT Capability (ISC) is an implementation of the SIGINT Database Application requirements within the existing INTEL FS Version 1.0 framework. It provides all of the features available from INTEL-FS Version 1.0 augmented with the integration of a SIGINT Analysis application and an integration with the NATO Emitter Database. ISC is a first class application within the INTEL FS framework and therefore leverages all of the existing INTEL FS framework capabilities. ISC supports all levels of command in the exploitation and analysis of SIGINT reporting provided by the SIGINT Contributing Nations.

Value Proposition: As a first class application within the INTEL FS framework the ISC leverages all of the existing INTEL FS capabilities plus for the SIGINT Analysis Domain includes support to:

- the Signals Intelligence component of all operational mission types;
- SIGINT reporting exploitation and analysis;
- SIGINT network and traffic analysis;
- Enhance collaboration and sharing in an environment dedicated to the SIGINT domain;
- development of none attributed, derived intelligence information entities and products;
- coordination with the broader Electronic Warfare community through the NATO Emitter Database;

Service Features: The INTEL FS SIGINT Capability offers the user:

- Compliant with policies, standards and requirements for installation and operation on SIGINT COINS at CTS-B including principles of none attribution and anonymity.
- Implementation of the SIGINT Domain Model in terms of SIGINT Intelligence Information Entities and Relationships.
- Management of SIGINT users, permissions and organisational administration.
- Synchronisation (low-to-high) with the broader ACO INTEL-FS intelligence repository.
- Automated processing of incoming SIGINT reporting – correlating contributions from all levels of NATO command and from the contributing SIGINT Nations.
- Automated generation of SIGINT reports.
- Integration with the NATO Emitter Database and the broader Electronic Warfare community.
- Support to SIGINT exploitation and analysis.
- Support to SIGINT network and traffic analysis.
- Development of none attributed intelligence information entities and products.
- Entity lifecycle management, discovery, search, archive, retrieval, dissemination, release and replication of SIGINT Intelligence Information Entities and Relationships.
- Workflow services; analysis views; a rich user interface; geospatial visualisation.

Service Flavours: The Service is available as a single flavour.

Available on:

- ISC is only available on SIGINT COINS which is a cryptographically isolated network.

Service Prerequisites:

- WPS001 - Managed Device Service

Standard Service Support Levels:

Service Availability[1] Target: 99.5% Availability
Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Instance.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

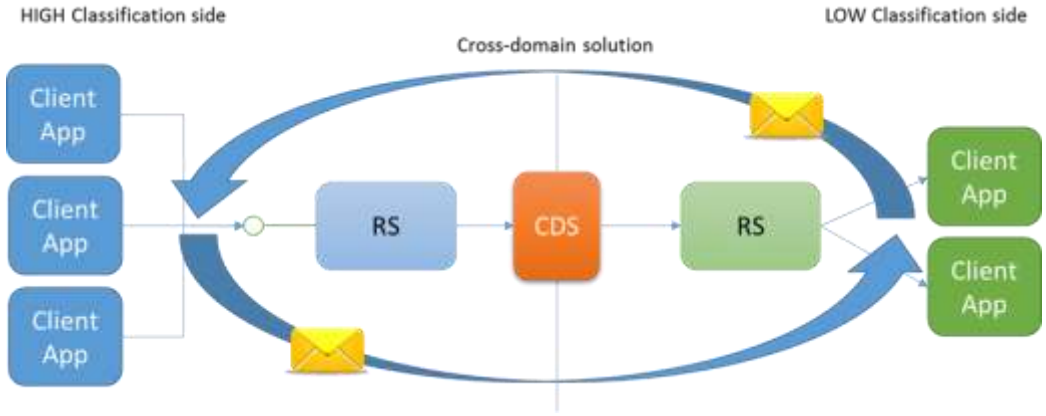
APP058 - Release Server (RS) Application Service

Service ID: APP058

Service Name: Release Server (RS) Application Service

Portfolio Group: Application Services

Service Description: The Release Server (RS) service interface provides an abstraction layer for applications to release information between two security domains of different security levels. The service hides the complexity of Cross Domain Solutions for client applications.



Value proposition: The RS provides a service interface for applications to release information between two security domains of different security levels. The complexity of cross domain solutions are hidden behind a simple service interface. The Release Server supports automated and controlled release of information (a man in the loop scenario).

Service Features:

The Application features:

* Configurable release rules based on release-ability markings (Authority, Classification and Release-ability);
* Automated or controlled (man in the loop) release of information;
* Monitoring;
* Fully Web based user interface;
* Fully documented;
* Automated installation package.

Support features:

* Support to implementation, integration and customization;
* Support to operations and maintenance;
* Support to training requirements;
* Information gathering for technical and training support. **Service Flavours:** The Service is available as a single flavour.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

Hardware:

- 64-bit architecture processor (multiple cores).
- Minimum 4 GB RAM (recommended 8 or 16 GB for operational use).
- 100 GB System drive.
- 500 GB Data drive minimum (depending on usage).

Software:

- MS Windows 2012 or newer
- IIS
- .NET Framework 4.6.2
- MS SQL Server 2008R2 or newer

The service can be configured remotely using a HTML5 compatible browser.

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP059 - Joint Exercise and Management Application Service

Service ID: APP059

Service Name: Joint Exercise and Management Application Service

Portfolio Group: Application Services

Service Description: The Joint Exercise Development and Management Application Service supports exercise scenario designers in developing the MEL/MIL (Master Event List/Master Incident List) for an exercise in a structured and deliberate manner according to the process specified in annex M of the Bi-SC Directive 75-3. The application service also supports an exercise control organisation in executing the MEL/MIL during an exercise in a collaborative, distributed and interoperable manner. The exercise observation and analysis process is also supported.

Value Proposition: This application service supports exercise scenario managers, control staff, observers and analysts in performing their tasks in the preparation and execution of an exercise in a distributed and collaborative manner. It adds value to the process of developing, executing, observing and analysing an exercise by:

- Providing support for a collaborative and distributed way of working during the preparation and the execution of an exercise MEL/MIL.
- Providing a structured way of describing the MEL/MIL according to the Bi-SC 75-3.
- Establishing an explicit relationship between training objectives and MEL/MIL
- Establishing explicit relationships between training objectives, observations and analysis
- Implementing a tailored workflow for the development and execution of a MEL/MIL.
- Implementing a tailored set of states for observations and analysis that are linked to training objectives.
- Providing in a single configurable view, the elements of exercise information that are critical to the implementation of specific roles in the exercise control organisation.
- Providing the ability to add new sources of exercise information without having to modify the exercise control business applications.
- Documented capability to rapidly build exercise control dashboards using regular office automation tools.

Service Features: The JEMM system is a web-based application that supports the collaborative and structured development, execution, observation and analysis of an exercise MEL/MIL. Specifically, JEMM offers the following features:

- Prepare and develop the MEL/MIL as specified in the Bi-SC 75-3 Directive.
- Prepare and describe the synchronisation with simulation-based or live support to the exercise.
- Manage the execution of the MEL/MIL
- Manage the synchronisation of activities with simulation-based or live support to the exercise.
- Prepare and manage the collection of observations by observer/trainers.
- Analyse the collected observations and assess the progress of training objective achievement.
- Assign roles and rights to various users to perform tasks relevant to their participation in the exercise.
- Tailor the workflow of the execution and observation processes.

- Document MEL/MIL, observations and analysis results.

In addition JEMM's Exercise Interoperability Service provides a structured and documented web-service and supporting management capability to configure heterogeneous exercise information providers. Exercise control business applications or regular office automation tools like Excel can connect to the EXIS web-service. The specific features are:

- A controlled and documented web-service that allows information providers to populate the service in a structured manner.
- A management interface that allows the user to configure provider information.
- A set of providers relevant for the NATO context: JTLS, JCATS, VBS, Excel, JOCWatch, ICC.

JEMM's reporting module supports the ability to generate a subset of AdAt-P3, and OTH-GOLD messages as well as tactical links according to Link 16 and NFFI standards from data provided through the exercise interoperability service.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
Mission Secret
PAN

Service Prerequisites:

WPS001 – Managed Devices Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP060 - ISR Coalition Shared Data (CSD) Service

Service ID: APP060

Service Name: ISR Coalition Shared Data (CSD) Services

Service Description: The Service supports a wide range of CSD-dependent customer facing applications (CSD clients), including Exploitation and IRM&CM applications, and Sensor Systems. Currently, supported applications are HMART, ICMT, and INTEL-FS, as well as national applications. The Service:

- enables the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) products through provision of a standard interface for storing, discovering, accessing and sharing heterogeneous ISR libraries maintained by NATO and Nations;
- provides workflow support to the overall JISR Process of Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) spanning multiple echelons, multiple military services and multiple NATO and national applications and services; and
- provides access to live or recorded Streaming Data types, such as Full Motion Video, Video Clips, or Ground Moving Target Indicator (GMTI) data

Portfolio Group: Application Services

Value Proposition: The Service supports the JISR systems, workflows, and processes in order to provide the right (intelligence) information, at the right time, in the right format and to the right location for commanders to make the right decisions.

Service Features:

Intelligence Surveillance Reconnaissance Coalition Applications features in the following categories:

- CSD ISR Product Library: storage, discovery, access and dissemination
- CSD ISR Workflow: support for JISR Collection Management and TCPED Process
- CSD ISR Streaming: access to live or recorded streaming data types

Supported JISR data formats, interfaces, and technical service contracts: STANAG 4545, STANAG 4609, STANAG 4607, STANAG 5516, STANAG 4559, and MAJIIC2 Bravo .1 Baseline.

Service Flavours: The Service is available in multiple flavours, depending on the combination of the following independent component services:

- ISR Product Library Services
- ISR Workflow Services
- ISR Streaming Services

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 - Managed device service

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP061 - Air Command and Control Information Services (AirC2IS) Application Service

Service ID: APP061

Service Name: AirC2IS

Portfolio Group: Application Services

Service Description: Air Command and Control Information Service (AirC2IS) is the Air Functional Service (including TBMD) of the Bi-Strategic Command Automated Information System (Bi-SC AIS) for all levels of the NATO Command Structure. It is a non-real-time Command and Control service, which provides the NATO air staff with an integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations (including Theatre Ballistic Missile Defence operations) in a responsive and timely manner. Together AirC2IS and Air Command and Control System (ACCS) provide NATO's complete Air C2 capability. AirC2IS is an integrated suite of applications that addresses the Air Command & Control (AirC2) requirements at the operational and strategic level, as specified in AJP 3.3(A). AirC2IS supports the NATO AirC2 cycle.

Value Proposition: AirC2IS is designed with the Operational Community for the Operational Community to address the following requirements:

- Web Based Access
- Expandability
- Flexibility and Customisation
- Interoperability and Collaboration
- Improved Usability
- Transition from Existing Systems

The AirC2IS provides the following values:

- Integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations in a timely manner.
- It is designed with a focus on collaboration and multi-system integration
- It ideally supports the operational level planning, assessment and information knowledge management processes
- Especially suited to the joint environment at static or deployed locations

Service Features: AirC2IS is able to access and send information from/to other functional mission areas (Land, Maritime, Special Operations Forces, Intelligence, Logistics, and others). To be able to do this, AirC2IS consumes information from and provides services to several systems, including ICC, NIRIS, LOGFAS, and NCOP.

Following functionalities are included in AirC2IS Increment 1:

Mission Applications:

- Interactive Map
- C2OA Manager
- ORBAT Applications
  - Generic Catalogue
  - Own ORBAT Manager
  - OPFOR ORBAT Manager

- Neutral ORBAT Manager
- TBMD Applications
  - OPFOR TBM COA Manager
  - PCAL Manager
  - JPCAL Manager
  - IDDM
  - SAWREP Manager
- Tactical Information Display
- CONOPS Manager
- Support to Air Logistics
- AOD Editor

Information Portal:

- HQ Portal
- Mission Portal

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

No	Service	Service Code	Version	BL4
1	ICC Application Service	APP049	2.7.4; 2.8.2	Yes
2	JTS Application Service	APP016	3.1	Yes
3	ACCS Application Service	APP050	N/A	Yes
4	NIRIS Application Service	APP010	3.7.1	Yes
5	SEW Application Service	APP002	2.1	Yes
6	NCOP Application Service	APP022	1.1.14; 1.1.15	Yes
7	LC2IS Application Service	APP017	1.1	Yes
8	LOGFAS Application Service	APP041	6.2	Yes
9	TOPFAS Application Service	APP007	5.0	Yes
10	JOIIS Application Service	APP008	8.3.5	Yes
11	JCHAT Application Service	APP015	Openfire 3.5.2; TCS 1.1.1	Yes
12	DHS (MS Share Point 2007)	APP031	2.1	Yes
13	CoreGIS Application Service	APP055	2.1.0	Yes

No	Service	Service Code	Version	BL4
14	EMS (SCCM, SCOM)	APP034	2012	Yes

Required to be in function prior to the service deployment.

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP064 - ITSM Toolset Application Service

Service ID: APP064

Service Name: ITSM Toolset Application Service

Service Portfolio Group: Application Service

Service Description: The ITSM Toolset Application Service provides the IT Service Management (ITSM) toolset required for connecting and automating processes underlying/enabling the management of the services provided by the NCI Agency. ITSM Toolset Service is an enabler of a unified platform and scalable architecture providing the foundations for managing services across their lifecycles. In particular, the Service drives the deployment of NCI Agency wide Service Management processes and service/system data collection with training and technical solutions, and provide the data warehouse for the NCI Agency Asset and Configuration Management capability and record keeping of all relevant information generated by the execution of the service management processes they support. As the Service Management requirements evolve, the toolset will be adapted according to the developing service catalogues and business requirements. In addition, ITSM toolset service provides the necessary means to mine in the wealth of collected data, identify and exploit relevant correlations; provide convincing information sharing, exploration and presentation means, while preserving information confidentiality on a need-to-know basis. Required Periodic Service Delivery, Availability and Service Quality Report use the collected data.

Value Proposition: The Service provides a centralised mean for effective and efficient management of services agreed in the SLA and enables the Service Quality Reports. It ensures that agreed processes and procedures are adhered, and identifies the issues and bottlenecks allowing continuous service improvement. It is a key control instrument for management of collects the necessary data to enable reporting of the achieved service levels, and therefore improves the overall effectiveness and productivity of the organisation.

Service Features: The features of the ITSM Toolset Service are: Request Fulfilment, Incident Management, Change Management, Problem Management, Asset & Configuration Management, Release and Deployment, Service Level Measurement and Reporting.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5%

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP065 - Joint Tactical Simulation (JCATS) Application Service

Service ID: APP065

Service Name: Joint Tactical Simulation (JCATS) Application Service

Portfolio Group: Application Services

Service Description: The Joint Tactical Simulation Application Service supports exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at a tactical level of decision-making. The tool used for the Joint Tactical Simulation service provides the Joint Conflict and Tactical Simulation (JCATS) system which is a US Government-Off-The-Shelf simulation application with a tailor-made interface application that supports the distributed and collaborative execution of training audience orders and exercise control guidance in a synthetic world. JCATS maintains the status of the synthetic environment and all represented joint forces in time and space.

Value Proposition: This application service supports exercise designers and control organisation in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training and its supporting command and control applications in a manner that is consistent in time and space based on the activities and capabilities of deployed forces. The application service allows the many contributors to the preparation and execution of a computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing support for tactical levels of information to meet the requirements of the exercise training audience.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Tactical Simulation Application Service offers the following features:

- Capture and manage detailed information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.
- Provides support to produce detailed information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.

In addition, the agency maintains a JCATS ORBAT Builder (JOB) application that supports exercise planners in building that part of the ORBAT for which they are responsible in a stand-alone manner in a format that is compatible with JCATS. An exported ORBAT file can be consolidated into a central JCATS exercise dataset by the exercise database developers.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret

Service Prerequisites:

WPS001 – Managed Devices Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The Service unit of measure is Per Instance.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP066 - The Joint Operational Simulation Application Service

Service ID: APP066

Service Name: The Joint Operational Simulation Application Service

Portfolio Group: Application Services

Service Description: The Joint Operational Simulation Application Service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at an operational level of decision-making. The Commercial-Off-The-Shelf simulation application adopted for this purpose is the Joint Theater Level Simulation (JTLS) with a web-based interface application that supports the distributed and collaborative execution of training audience orders and exercise control guidance in a synthetic world. JTLS maintains the status of the synthetic environment and all represented joint forces in time and space.

Value Proposition: The Joint Operational Simulation Application Service supports exercise designers and control organisation in gathering and managing all the detailed synthetic data that is required to realistically produce information flows towards the training and its supporting command and control applications in a manner that is consistent in time and space based on the activities and capabilities of deployed forces. The application service allows the many contributors to the preparation and execution of a computer-assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing interoperability with NATO command and control systems in an efficient and flexible manner.
- Providing support for operational levels of information detail to meet the requirements of the exercise training audience.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Operational Simulation Application Service offers the following features:

- Capture and manage aggregated information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.
- Provides support to produce aggregated information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.
- Interfaces to a number of NATO C2 systems.

Service Flavours: The service is available as a single flavour.

Available on:

Mission Secret

Service Prerequisites:

WPS001 – Managed Devices Service

Standard Service Support Levels:

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP069 - Air Integrated Training Capability (ITC) Application Service

Service ID: APP069

Service Name: Air Integrated Training Capability (ITC) Application Service

Portfolio Group: Application Services

Service Description: The Air Integrated Training Capability (ITC) Application Service supports air commands exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world. In addition the service supports the exercise control organisation in generating relevant and compatible information flows to the training audience automated air command and control systems and in extracting structured order information from those systems.

Value Proposition: ITC application service supports exercise designers and control organisation in the air C2 community in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training audience and its supporting Air C2 systems. The application service allows the many contributors to the preparation and execution of an Air C2 computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner using a familiar interface.
- Providing interoperability with NATO Air command and control systems in an efficient and flexible manner.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.

Service Features: The ITC system is built upon a Commercial-Off-The-Shelf simulation framework (FLAMES). ITC provides an air exercise control organisation with the ability to simulate air operations as defined in an Airspace Coordination (ACO) and Air Tasking Order (ATO) for two opposing and one neutral side. An exercise controller can manage the overall execution of the scenario and influence the adjudication of simulation outcomes. The resulting status updates are fed automatically into the Integrated Command and Control (ICC) in the form of air tracks, status updates and messages.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret

Service Prerequisites:

WPS001 – Managed Devices Service

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning

- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP070 - Training Objective Development and Management (TOMM) Application Service

Service ID: APP070

Service Name: Training Objective Development and Management (TOMM) Application Service

Portfolio Group: Application Services

Service Description: The Training Objective Development and Management Application Service supports exercise training audiences and associated training organisations in producing a structured and prioritised set of training objectives for a particular training event and phase in a collaborative and distributed manner according to the process in the Bi-SC Directive 75-3 Annex V.

In addition, the application service supports exercise training audiences and associated training organisations in managing training objective resource conditions in a distributed and collaborative management according to the guidance described in the Bi-SC Directive 75-3 Annex V throughout the exercise preparation phase.

Value Proposition: This application service supports exercise training objective owners and supporting resource condition owners in developing training objectives according to the Bi-SC Directive 75-3 in a structured manner. It adds value to the process of developing and managing training objectives by:

- Providing support for a collaborative and distributed way of working.
- Providing support for the workflow between the stages of development.
- Providing an explicit statement of resource requirement and acknowledgment by resource owner.
- Providing a real time up to date dashboard of the state of achievability of training objectives throughout the exercise planning and preparation process
- Reducing travel and coordination effort.
- Enabling a wider participation in the process by training audience personnel and resource owners.

Service Features: The features of the Training Objective Management Module (TOMM) are:

- Act as a Training Objective Manager capable of managing the contributions and workflow of the TO development process including the prioritisation
- Act as Training Objective Scripter capable of defining the content of training objectives, the associated resourcing conditions and standards
- Act as a resourcing condition owner capable of commenting and acknowledging resource requirements.
- Develop training objectives according to the stages and format specified in the Bi-SC Directive 75-3 Annex V.
- Review training objectives and associated resource conditions in a collaborative and distributed manner
- Manage and track the achievability state of the training objective resourcing conditions.
- Prioritise training objectives and re-organise their sequence accordingly.
- Review and update the achievability of resource conditions in a dashboard until the start of the exercise.

Service Flavours: The Training Objective Development and Management (TOMM) Application Service is offered as a single standard flavour.

Available on:

Mission Secret

Service Prerequisites:

WPS001 – Managed Devices Service

Standard Service Support Levels:

Service Availability[1] **Target:** 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Instance.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

This page is left blank intentionally

SECURITY SERVICES

V3.4

This page is left blank intentionally

SEC001 - Security Accreditation Support Service

Service ID: SEC001

Service Name: Security Accreditation Support Service

Portfolio Group: Security Services

Service Description: The Security Accreditation Support Service provides guidance and support for security accreditation and re-accreditation activities for active and pipeline services, including the preparation of documentation required to support Security Accreditation.

Value Proposition: Support to Cyber Security - Assessment. This service enables the reduction of security risk to the NCI Agency, ensuring Cyber Security Policies, Architectures and Acquisition strategies, internally and externally, are coherent and effective. Additionally it provides assurance and stability of a well understood regulatory framework by all stakeholders.

Service Features: Security Accreditation Support Service is comprised of the following elements:

Security Accreditation Preparation and Documentation (New Systems): Extracting and formatting from the results of the Security Design to the Security Accreditation Templates and other supporting documentation such as Security Risk Assessment (SRA), System-specific Security Requirements Statements (SSRS), and SecOPs. Serves as first Point-of-Contact for Accreditation of new systems.

Security Accreditation Support (In-service systems): Comprehensive coordination with the NATO CIS Security Accreditation Board (NSAB) or any applicable Security Accreditation Authority (SAA). Guidance and support on security accreditation and re-accreditation activities as required by the NATO SAA's. Interfacing to the NSAB or applicable SAA, the security-related documentation. Assistance to the Security Accreditation Authorities, to review and provide technical assessment of the security-related documentation, required in the accreditation process for CIS introduced or managed by other than the NCI Agency. Development of security accreditation strategies. Serves as first Point of Contact for re-accreditation of in-service systems.

CIS Security Conformity Support: Support towards formal attestation that the prescribed security measures are in place. This ensure that new or modified security services meet the security expectations of the customer as well as the requirements of the NATO Security policy and supporting Directives before being deployed and activated.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC002 - Cyber Security Assessment Service

Service ID: SEC002

Service Name: Cyber Security Assessment Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Cyber Security Assessment Service seeks to assess compliance to standards and identify vulnerabilities, through the online or onsite analysis of CIS, websites, customer sites and communication equipment, in order to allow remediation to occur.

Value Proposition: Support to Cyber Security - Assessment. Principally this service enables the customer to have a better understanding of their vulnerabilities and so be able to remediate them before being exploited. Being able to understand any vulnerabilities and strengths also supports being able to build a picture of overall security, creating a baseline for measure progress to security improvements.

Service Features:

Online Vulnerability Assessment and Remediation Support: Provision of Enterprise Online Vulnerability Assessment resources to carry out continuous and dynamic evaluations / audits of CIS infrastructures / systems to identify any vulnerabilities in software or configurations and to provide detailed reports. Includes the conduct of the following checks:

- Inventory of all connected devices
- Inventory of authorized and unauthorized software (limited functionality)
- Inventory of patch and update status of all installed software and operating systems (limited functionality)
- Secure configurations for hardware and software on workstations and servers (limited functionality)
- Malware defences (limited functionality)
- Secure configurations for locally managed network devices (limited functionality)

Remediation Support: Processing 30 day follow up sheet replies. Advising on mitigation techniques, escalating issues and closing vulnerabilities at sites.

On-Site Vulnerability Assessment (Type 3-5 Security Audits) and Remediation Support: NATO Type 3 Security Audit: Provision of resources to carry out COMPUSEC checks on NATO CIS to ensure compliance with NATO CIS security policies, directives and guidance documents including NCIRC TC Security Guidance and Caveats to approved CCPs. Includes the conduct of the following checks:

- Inventory of all connected devices
- Inventory of authorized and unauthorized software
- Inventory of patch and update status of all installed software and operating systems
- Secure configurations for hardware and software on workstations and servers
- Malware defences
- Secure configurations for locally managed network devices
- Controlled use of administrative privileges
- Controlled access based on the need to know principle
- Data loss prevention

- Locally managed boundary defence.

NATO Type 4 Security Audit: Provision of resources to evaluate the security of computer systems or networks by simulating an attack from malicious outsiders or insiders and to provide detailed reports about the findings.

NATO Type 5 Security Audit: Provision of resources to evaluate the security of computer systems or networks by simulating an attack from malicious outsiders or insiders with no notification to personnel other than unit commander and security officer and to provide detailed reports.

Industrial Control Systems Building Management Systems (Discretionary): Specialist VA of ICS with findings and remediation recommendations are provided with the assessment report.

Cyber Hygiene Management and Post Audit Remediation Services:

- Processing 30 day follow up sheet replies. Advising on mitigation techniques, escalating issues and ensuring the closure of vulnerabilities at sites
- Provision of resources to carry out on-site remediation activities

Online Vulnerability Assessment and Reporting:

- Provision of Enterprise Online Vulnerability Assessment resources to carry out continuous and dynamic evaluations / audits of CIS infrastructures/systems to identify any vulnerabilities in software or configurations and to provide detailed reports.

Website Vulnerability Assessment: Provision of resources to assess internet facing web sites for security mis-configuration, vulnerabilities and coding bad practices. The findings and remediation recommendations are provided with the assessment report.

TEMPEST Facility Zoning: Provision of electronic evaluation of Facilities and Buildings where Classified information is processed in order to determine their Facility Zone Rating. Including advice to local IA staff on TEMPEST issues. The zone rating is provided with a technical report.

EMSEC Vulnerability Assessment: Provision of EMSEC vulnerability assessment within a Zoned Facility. The service includes advice to local IA staff on TEMPEST issues. The findings of the assessment is provided as a report.

Equipment TEMPEST Level Testing: Provision of Equipment TEMPEST Level Testing service. The result of the testing is provided as a report.

TRANSEC Vulnerability Assessment: Provision of real time monitoring of an organisation's non secure communications (GSM, analogue, digital and VoIP), with the purpose of presenting realistic and effective countermeasures to limit the disclosure of intelligence information to unauthorised personnel/agencies. The result is provided with an assessment report.

TRANSEC Awareness: Provision of TRANSEC awareness training/briefings to include IA OPSEC/TRANSEC Awareness, including Roadshows.

Service Flavours: The Service is available as a single flavour.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC003 - CIS Components Analysis, Supply Chain Trustworthiness, and Risk Assessment Service

Service ID: SEC003

Service Name: CIS Components Analysis, Supply Chain Trustworthiness, and Risk Assessment Service

Portfolio Group: Security Services

Service Description: The CIS Components and Supply Chain Trustworthy Analysis Service provides assessment to CIS components and their trustworthiness. This service provides analysis and evaluation on the reliability of CIS components and the trust that can be placed upon them. Coordination in Security Risk Assessment Working Groups supports, leads, or coordinates Security Risk Assessment Working Groups for NATO programmes or projects.

Value Proposition: Support to Cyber Security - Sustainment. CIS Components and Supply Chain Trustworthiness analysis enables the deployment and operation of CIS infrastructure with an understood level of trust. This allows the appropriate management of risk to the confidentiality, integrity and availability of communications and information. Coordination in Security Risk Assessment Working Groups leverages specialist knowledge of cyber risk to enable NATO risk assessment.

Service Features:

CIS component Cyber Security: Analyse and evaluate the extent to which one can rely on a CIS component, be it hardware, software, or both, to function as intended. The assessment can be made through either a set of assurance techniques or less rigorous means.

Supply Chain Cyber Security: Plan for, collect information about, assess, and handle the level of trust that can be placed in the components of a CIS based on the supply of sub-components, manufacturing, and logistics.

Coordination in Security Risk Assessment Working Groups: Support, lead, or coordinate Security Risk Assessment Working Groups for NATO programmes or projects. This includes lead or coordinating the meetings and ex-committee work, providing advice regarding security risk assessment and risk management process, and support conducting SRA by the Group. Specifically for the NATO Security Risk Assessment Group (NSRAG) this services entails the review and approval (in coordination with SAAs) of the specification of risk assessment/management tools used for NATO CIS (e.g. NATO profile for PILAR), the development and maintenance of generic security risk assessment for NATO CIS scenarios as well as support of NOS and the Security Committee in IA format in the review / development of NATO documents addressing security risk assessment / management and provision of support to NSAB.

Security Test and Verification (ST&V): Pre-Production Security Testing Security Testing and Consultancy services conducted in support of Change Management (CCP) and accreditation processes, for projects includes: documentation review, vulnerability assessment and penetration testing.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified

NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC004 - Cyber Security Analysis Service

Service ID: SEC004

Service Name: Cyber Security Analysis Service

Portfolio Group: Security Services

Service Description: Cyber Security Analysis Service provides CIS Forensics and Malware analysis which are conducted to better understand security threats, to support the understanding, mitigation, remediation of incidents and to gather evidence.

Value Proposition: Support to Cyber Security - Defence. This service provides greater insight into potential security threats that contribute to lowering business risks. Furthermore informing better future prevention strategies obtained through a deep understanding of the nature of malware and forensic analysis.

Service Features: Cyber Security Analysis Service is comprised of the two following elements:

- Forensic Analysis: Provision of resources to perform online (OCF) and stand-alone (SCF) computer forensics analysis for Incident Management and on-request.
- Malware Analysis: Provision of resources to carry out technical analysis on suspicious application code to identify any malicious content. Sharing of technical characteristics of malware within a trusted community either on an *ad hoc* basis or via an automated MISP platform.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites: Online analysis requires the provision of resources to ensure that all NCIRC Operational Applications are maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, performance tuning And connectivity to NS, NR, NU, MS.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC005 - NATO Cyber Defence Rapid Reaction Team Service

Service ID: SEC005

Service Name: NATO Cyber Defence Rapid Reaction Team (RRT)

Portfolio Group: Security Services

Service Description: The NATO Cyber Defence RRT provides rapid, technical cyber defence assistance to NATO organisations and to individual NATO Allies subject to Council decision (on a case by case basis). The RRT's foundation is the provision of 2 x teams of NATO cyber experts but it can reach into NCI Agency's staff for deep expertise in order to deploy capabilities similar to those of the NCIRC TC , but at remote locations and in response to Cyber Security incidents and crises.

Value Proposition: Support to Cyber Security – Defence. The Cyber Defence RRT provides flexible, deployable Cyber Security response where in times of crisis.

Service Features: The NATO Cyber Defence RRT is comprised of the following elements:

- Digital Forensics
- Malware Analysis
- Event/security Log collection
- Intrusion Detection System
- Full Packet Capture
- Online Vulnerability Assessment
- Incident Management

Service Flavours:

Deployed
Distributed
Centralized (NCIRC TC) response

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC006 - Cyber Security Incident Management Service

Service ID: SEC006

Service Name: Cyber Security Incident Management Service

Portfolio Group: Security Services

Service Description: Cyber Security Incident Management Service provides COMSEC and COMPUSEC Incident, Violation and Insecurity Investigation. The service enables an effective and efficient response to immediately contain a detected and/or reported Incidents, including incident containment, eradication, recovery and follow-up.

Value Proposition: Support to Cyber Security – Defence. This service provides a centralised Incident Handling and Response. The experienced, effective and efficient management of identified incidents through Cyber Security Incident Management Service ensure correct handling through incident lifecycle, in turn strengthening cyber security capability and therefore the overall effectiveness and productivity of the organisation.

Service Features: The service is comprised of: Incident Triage; Event Correlation; Incident Handling & Response; Alerting, Reporting, and Assisting with Recovery; Incident Analysis and Follow-up; and Monitoring, Evaluating and Recovering from COMSEC incidents, violations and insecurities.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

On-site support, including logistical, security, technical and political coordination.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC007 - Cyber Security Monitoring Service

Service ID: SEC007

Service Name: Cyber Security Monitoring Service

Portfolio Group: Security Services

Service Description: The Cyber Security Monitoring Service provides the monitoring of networks, websites and email traffic to detect and identify threats and compromises, and so to ensure cyber security.

Value Proposition: Support to Cyber Security – Defence. This service is designed to detect incidents – as a prerequisite to incident response. By monitoring millions of events each day, the Cyber Security Monitoring Service delivers better cyber security of NATO CIS by provides assurance that:

- Email data spillages are detected and minimised
- Monitored website in question is available and undefaced
- Events will be correlated and scrutinised by qualified and experienced Security Analysts for appropriate actions as required

Service Features: This service is comprised of the following elements:

- Internet Facing E-Mail Content Monitoring: The provision of the ability to check all Inbound/Outbound Internet e-mail to ensure compliance with NATO and applicable local Security Polices; such checks include malicious code, executable content, encrypted content, SPAM, and Classified Data content. Outbound e-mail can be monitored either centrally by the NCIRC TC, or locally by appropriate IA Staff.
- Internet Web Site Monitoring: The ability to centrally monitor customer's Internet-facing Web Sites for unauthorised changes and to take appropriate reporting/remedial actions.
- Network Monitoring: Network Intrusion Monitoring, Detection & Prevention is the provision of centrally managed and monitored Network-based technologies:
  - Intrusion Detection Systems (IDS) – will detect, log, and report network-based malicious activity.
  - Intrusion Prevention Systems (IPS) – as for IDS with the additional function of the ability to attempt to stop/block detected activity.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

SEC011 – Gateway Security Service
Provision of resources to ensure that all NCIRC Operational Applications are installed and maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, and performance tuning.

Provision outage and change notifications in order to minimise false-positives.

Standard Service Support Levels:

Service Availability Target: N/A

Service Restoration: 2 business days.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC008 - Cyber Security OPCEN Helpdesk Service

Service ID: SEC008

Service Name: Cyber Security OPCEN Helpdesk Service

Portfolio Group: Security Services

Service Description: NATO Cyber Security Helpdesk provides the customers the single point of contact for cyber security related incidents, requests and advice as well as cryptographic equipment configuration and keying.

Value Proposition: Support to Cyber Security – Defence. Continually accessible advice and action to support the customer in the maintenance of efficient and compliant cyber security and cryptography that underpins the security of our communication and information.

Service Features: This service provides a 24/7 presence of specialists to give advice on potential cyber security incidents (and appropriate escalations as required), cryptographic equipment installation, configuration, keying, operation, trouble shooting and related technical or engineering issues, production of user configuration data sheets and user documentation for IP encryption devices.

Service Flavours: The Service is available as a single flavour.

Service Available on:

RS MS
RS NS
NSV2
NNCCRS
SIGINT COINS
NRF MS
NRF NS
SACEUR VTC
NAEW

Service Prerequisites:

None

Standard Service Support Levels: TBD

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC009 - Cyber Security Awareness and Outreach Service

Service ID: SEC009

Service Name: Cyber Security Awareness and Outreach Service

Portfolio Group: Security Services

Service Description: Cyber Security Awareness and Outreach Service:

- Supports outreach in order to support CS SL development and, where appropriate, broader NATO Cyber Security aims. Encourages liaison and information sharing through outreach programmes and distribution of regular Cyber Security reporting, including Vulnerability Assessments and Cyber Sitreps. Outreach, including contribution to Cyber Sitreps, briefings, portals and other information campaign activities.
- Risk Communication and Education: Educate all relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Value Proposition: Support to Cyber Security – Inform. This service enables improved cooperation between Cyber security entities, better representation of cyber security domain and improved representation of Cyber security requirements and priorities. Risk Communication and Education educates relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Service Features: This service is comprised of the following features:

- **Cyber Security Outreach:** Supporting outreach in order to support CS SL development and, where appropriate, broader NATO Cyber Security aims. Encouraging liaison and information sharing through outreach programmes and distribution of regular Cyber Security reporting. Outreach, including contribution to stakeholder engagement, briefings, contribution to NATO Cyber Training, portals and other information campaign activities.
- **Risk Communication and Education:** Educate all relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Service Flavours: This Service is available as a single offering.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC010 - Cyber Security Information Sharing Service

Service ID: SEC010

Service Name: Cyber Security Information Sharing Service

Portfolio Group: Security Services

Service Description: Cyber Security Information Sharing and Reporting is the communication of specific, timely and authoritative guidance.

Value Proposition: Support to Cyber Security – Inform. The sharing of timely and accurate information is essential to maintain the cyber security strength of the organisation, as a proven way forward to increase/maintain security posture.

Service Features: Bulletins (including NIMBL), briefings, operational reporting, portals and other communications with Cyber Security communities of interest. Generation of reactive advisories to mitigate discovered vulnerabilities or to reduce the impact of newly emerged threats.

Service Flavours:

Cyber Defence Information Sharing: An extended service from the Malware Information Sharing Platform (MISP), covering Cyber Defence-relevant information (e.g. threats, vulnerabilities).

Cyber Defence Information Sharing Capability (CDIS – see [NCIA TR/2014/SPW009346/04, 2016]) currently not available.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC011 - Gateway Security Service

Service ID: SEC011

Service Name: Gateway Security Service

Portfolio Group: Security Services

Service Description: Gateway Security Services provide a secure interconnection of different networks or network sections in order to protect an organization's key information. Service is comprised principally of Data Diodes, Firewalls, Guard, Mailguard and VPN.

Value Proposition: Support to Cyber Security - Prevent. Expert and effective Gateway Security management is a fundamental cyber security requirement, preventing compromise and facilitating secure connectivity.

Service Features: This service is comprised of the following elements:

Gateway Security VPN Services:

- Central management and configuration of VPN Gateways
- Provisioning of centrally managed VPN Gateways
- Monitoring, updating and patching of centrally managed VPN Gateways
- Client-to-Site VPN
- Site-to-Site VPN
- Configuration Backup
- Disaster Recovery Services
- Log forwarding to archiving and/or forensic systems
- Back-reporting of system health issues

Gateway Security – Mailguard Services:

- Central management and configuration of Mailguard
- Provisioning of centrally managed Mailguard
- Monitoring, updating and patching of centrally managed Mailguard
- Configuration Backup
- Disaster Recovery Services
- Log forwarding to archiving and/or forensic systems
- Back-reporting of system health issues
- End-user support to identify mail rejection issues

Gateway Security – Firewall Services:

- Central management and configuration of Firewalls
- Provisioning of centrally managed firewalls
- Monitoring, updating and patching of centrally managed firewalls
- Configuration Backup
- Disaster Recovery Services
- Log forwarding to archiving and/or forensic systems
- Back-reporting of system health issues

Gateway Security - Guard Services:

- Central management and configuration of XML-Guard Services

- Provisioning of centrally managed XML-Guards
- Monitoring, updating and patching of centrally managed XML-Guards

Gateway Security - Data Diode Services:

- Central management and configuration of Data Diode Systems
- Provisioning of centrally managed Data Diode Systems
- Monitoring, updating and patching of centrally managed Data Diode Systems
- Configuration Backup
- Disaster Recovery Services
- Log forwarding to archiving and/or forensic systems
- Back-reporting of system health issues

Proxy services

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

Gateway Security Services depend on the installation of appropriate network infrastructure.

Standard Service Support Levels:

Service Availability: 24/7

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC012 - CIS Protection Support Service

Service ID: SEC012

Service Name: CIS Protection Support Service

Portfolio Group: Security Services

Service Description: Provision of expert guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software. This guidance is used to harden NATO CIS against attack and compromise.

Value Proposition: Support to Cyber Security – Prevent. The provision of CIS Protection Support enables coherent implementation of enterprise-wide endpoint security software, aligned to the policies and requirements of NATO that hardens the NATO CIS against compromise and is a proven way forward to increase/maintain security.

Service Features: The use of deep, niche expertise to deliver guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software.

Service Flavours: The Service is available as a single flavour.

Service Available on:

Network neutral

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC013 - Crypto Compliance Support Service

Service ID: SEC013

Service Name: Crypto Compliance Support Service

Portfolio Group: Security Services

Service Description: Crypto Compliance Support Service provides assessment for Crypto Logistic Support and Maintenance and COMSEC Account management. It does this by providing formal inspections of all organisations storing, operating or maintaining NATO funded cryptographic equipment and NATO COMSEC Accounts in order to ensure compliance with established Directives.

Value Proposition: Cyber Security – Assess. Compliant cryptographic and communication security underpins the cyber security required within NATO and within the Allies. This service provides assurance that cryptographic installations are compliant with appropriate directives procedures and practices of COMSEC account custodianship are compliant with appropriate directives.

Service Features: The Service is comprised of the following elements:

> **Crypto Logistic Support, COMSEC Account and Maintenance Inspections**: Provision of formal inspection of all organisations storing, operating or maintaining NATO funded cryptographic equipment in order to ensure that the procedures and practices of account custodianship, cryptographic logistic support, installation and maintenance is compliant with established Directives.

Service Flavours: The Service is available as a single flavour.

Service Available on:

> NATO Secret
> Mission Secret

Service Prerequisites:

> Appropriate crypto and network access authority.

Standard Service Support Levels: N/A

Support Hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.00 Fri 08.30-15.00 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC014 - Crypto Management and Logistic Support Service

Service ID: SEC014

Service Name: Crypto Management and Logistic Support Service

Portfolio Group: Security Services

Service Description: This service delivers management and logistic support required to securely implement and operate NATOs crypto solutions. This includes the management of the CARDS, EKMS, NEKMS, DEKMS and Data at Rest IA Services, the Operational Control of the Crypto Forward Support Points and Cryptographic Keying Material Distribution and expert Device Procurement Support.

Value Proposition: Support to Cyber Security – Prevent. Reliable management of crypto forward support. Delivery of authoritative functional, cryptographic expertise. Enabling of policy compliance and security, and the confidentiality, integrity and availability of data at rest.

Service Features:

CARDS, EKMS, NEKMS and DEKMS Services:

- Provision of resources to deliver the NATO wide accountability, receipt, transfer, supersession and destruction of cryptographic keying material and equipment.
- Maintenance of the CARDS Servers and authorisation for CARDS access to COMSEC custodians.
- Provision of specialist advice on cryptographic equipment installation, configuration, keying, operation, trouble shooting and related technical or engineering issues.
- Provision of the main point of entry for DACAN Electronic Key Management System (DEKMS) into NATO. Interface for DEKMS to NATO EKMS (NEKMS) for NATO wide distribution of crypto electronic keys.

Data at Rest IA Services: Provision of NATO Offline Crypto Equipment (NOLCE) keying Authority. Distribution and keying of all NATO Offline systems (Eclypt, SIR, Flagstone, etc.).

Crypto Management and Logistic Support

- Cryptographic Device Procurement Support
  - Advice on the design scope and planning for the procurement of NATO-approved cryptographic solutions, and execute the procurement and potentially provide the related services: implementation, training and maintenance.
- Operational Control of the Crypto Forward Support Points.
  - Provides Operational Control and Management of the Crypto Forward Support Points NATO-wide. Provision of timely replacement equipment and testing of faulty equipment prior to evacuation into the maintenance chain.
- Cryptographic Keying Material Distribution
  - The timely distribution of operational keying material and equipment to the end-user.
  - Allocation of keys to service requests (SRTS).
  - Provision of Controlling Authority services for all operational (theatre) and most operational (non-theatre) physical and electronic keying material.
  - Centralised management of distributed Crypto IP equipment providing the encryption of classified data (up to CTS level).

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Secret
Mission Secret

Service Prerequisites:

Appropriate crypto and network access authority. Maintenance, repair of Crypto Equipment. Replacement of faulty crypto equipment on operational circuits. NATO wide Crypto delivery, accounting and key distribution system. The Data at rest IA Service is dependent on available and trained staff to operate, distribute crypto material.

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC015 - Security Certificate Service

Service ID: SEC015

Service Name: Security Certificate Service

Portfolio Group: Security Services

Service Description: Provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities, including the appropriate training of registration authority personnel.

Value Proposition: Support to Cyber Security – Prevent. Secure connection and to authentication through digital certificate creation and management.

Service Features:

Certificate Authority Services for NS / MS, NU / NR and NMS: A service used for the creation and issuance of digital certificates to end-user (both human and non-human). This is service will be provided from a Registration Authority (RA). The RA will be only interface to the NATO PKI system to create and issue digital certificates. The service provided also includes the revocation process. RA's will be installed locally to provide services to the end user both human and non-human. Manpower to operate Registration Authorities situated outside of the NATO Command Structure is not included within this service line. Manpower to operate Registration Authorities for non-eligible entities or exceptional-eligible entities not co-located with a NCS sites shall be provided by those external agencies or multinational entities.

Revocation services to NS / MS, NU / NR and NMS: CRL and OCSP services to NS/MS, NU/NR and NMS is a service used for providing a valid Certificate Revocation List and OCSP responses to end users, both human and non-human. The CRL provides a list of revoked certificates, this list will be checked, every time an end user uses digital certificates to establish a secure connection, or to authenticate to a system the CRL is checked. As soon as a certificate is on the CRL the connection, authentication is denied. OCSP responses provide the validity of a single end entity including the full chain in response to a specific query. The OCSP and CRL services to the aforementioned networks are a vital and critical service.

Lifecycle Management of Digital Certificates / Entities: Lifecycle Management of Digital Certificates / Entities is a service which contains the creation, issuance, management, maintenance, re-issuance, key recovery, revocation and deletion of a bonafide end-user (both human and non-human). The lifecycle management of digital certificates / entities also includes the partial management, maintenance of the meta directory on which the user are created.

Training of Registration Authority Personnel: Training of Registration Authority personnel is a service used for on the job training of Registration Authority Operators (RA Operators). On the job training takes place after the local site received a RA and the RA is configured and operational.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NMS

Service Prerequisites:

The connectivity to the Certificate authority on the desired network. The system is also dependent on available and trained staff to operate the RA.

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC016 - Cyber Security Capability Development SME Service

Service ID: SEC016

Service Name: Cyber Security Capability Development SME Service

Portfolio Group: Security Services

Service Description: This service combines a number of subservice flavours, each of which provide specialist Capability Development SME capabilities, principally supporting sustainment activities.

Value Proposition: Support to Cyber Security - Sustainment. Centralised SME services offer good value by combining the synergies of collocated deep skillsets with the efficiency of having cyber specialists available and resourced only when the customer requires them to contribute to cyber security sustainment and capability development.

Service Features: This service provides flexible and bespoke Cyber Security SME solutions and Cyber Security Support comprising:

- CIS Project Cyber Security Research and Consultancy
- Security Setting Configuration Consultancy
- Cyber Security Design Services
- Cyber Security Education and Training Support Services
- Cyber Security Architecture Services
- Cyber Security Policy Support
- Cyber Security Tool Selection

Service Flavours:

CIS Project Cyber Security Research and Consultancy: Consultancy on security aspects of implementation, configuration, management and support of NATO CIS software, systems and devices. Includes CIS Security Data Mining & Business Intelligence and Cyber Security Business Continuity Planning Consultancy. Research CIS Security systematically investigates areas related to CIS Security in order to establish new technologies and approaches that can improve CIS Security.

Security Setting Configuration Consultancy: Provision of security configuration settings for in-use and future CIS Applications, software, Networking devices and Operating Systems software. Provision of configuration guidance for the securing of Boundary Protection devices, to include the approval of information flows over those devices as part of the configuration change process or firewall rule base change request process.

Cyber Security Design Services: Design CISs that are able to adapt to changing conditions in order to accomplish appropriate levels of CIS Security. Incorporates Vulnerability Assessment services as required. Adopt or develop CIS Security designs that can be implemented efficiently and that fulfil CIS Security requirements. Derive adequate CIS Security requirements and measures for systems or networks by valuating assets in the presence of known threat environment and vulnerabilities. It includes the analysis the security risk induced by the implementation of a new capability, a change to an existing one or systems that are delivered and are about to go operational. May include provisioning of Value analysis (potentially offered separately).

Cyber Security Education and Training Support Services: Provide technical and policy aspects of guidance on Cyber Security Education and Training guidance (i.e., Training Needs Analysis).

Cyber Security Architecture Services: Definition of security focussed mission and NCI Agency enterprise objectives, expectations, and responsibilities. Review of overarching (high level) architectures and target architectures ensuring compliance to NATO Security Policies and architectural coherence among projects and systems. Support to establish this strategic direction is provided as requested and coordinated by SSTRAT.

Security Architecture (Adoption): Provide adequate organization of CIS security requirements into a security architecture for any CIS system in order to ensure efficient usage of security resources aligned with high-level direction and guidance. This entails the CS support on overarching, reference, and target architecture for every introduced NATO capability.

Cyber Security Policy Support: Support the development and maintenance of technical NATO Directive and Guidance documents, and review of Cyber Security/Information Assurance/Cyber Defence related documentation. This covers both documentation through the NOS Roadmap as well as any supporting documents in NATO's regulatory security framework. Support to NATO Policies' and high-level Directives' Development. This includes NATO Security Policy, NATO Information Management, NATO Cyber Defence Policy and all applicable Enclosures.

Cyber Security Tool Selection: Development of guidance in the selection of specific CIS security tools. Support and advice on Information Assurance products evaluation and certification. This service may support the maintenance of the NATO Information Assurance Product Catalogue (NIAPC).

Available on: Network neutral

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC017 - Crypto Assessment Support Service

Service ID: SEC017

Service Name: Crypto Assessment Support Service

Portfolio Group: Security Services

Service Description: This service delivers integration and validation required to securely implement and operate NATOs crypto solutions. The activities within this service range from site surveys, equipment installations, testing and inspections to training and management support.

Value Proposition: Support to Cyber Security – Assess. Reliable management of crypto forward support. Delivery of authoritative functional, cryptographic expertise.

Service Features:

Cryptographic Integration Services:

- Installation Site Survey: Provision of Initial Site Surveys in order to deliver specialist implementation and physical security advice prior to installation of cryptographic equipment or implementation of systems with a cryptographic component.
- Cryptographic Equipment Installation: Installation of Cryptographic Devices within Alliance and also individual Nations for end to end encryption ensuring installation and operation complies with current regulations, standards and directives. Installation of all types of cryptographic equipment, to include Voice, IP, Link, Trunk and Wide-Band.
- Production of IP Data Configuration Sheets: Production of user configuration data sheets for IP encrypted links.
- CIS System Management Support: Support to NCI Agency System Managers (and others) in the location, installation and on-site trouble shooting of systems, which include, but are not limited to, NNCCRS, SIGINT COINS, NNPS, NSWAN.

Cryptographic Validation Services:

- Installation Inspection: Provision of installation compliance inspections and/or advisory visits on cryptographic installations in order to ensure compliance with current regulations, standards and directives.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

Appropriate crypto and network access authority. Maintenance, repair of Crypto Equipment. Replacement of faulty crypto equipment on operational circuits. NATO wide Crypto delivery, accounting and key distribution system.

Standard Service Support Levels:

Service Availability Target: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC018 - Cyber Security Project Management Service

Service ID: SEC018

Service Name: Cyber Security Project Management Service

Portfolio Group: Security Services

Service Description: Conduct and management of projects and programmes according to PRINCE2 methodology. This service includes the definition of acquisition requirements and contracting strategy, followed by a competitive outsourcing to industry from the 29 NATO nations. It includes as well partnering with industry to ensure that the latest, state-of-the-art technology is implemented in a coherent and cost-effective way.

Value Proposition: Support to Cyber Security - Sustainment. Centralised SME services offer good value by combining the synergies of collocated deep skillsets with the efficiency of having cyber specialists available and resourced only when the customer requires them to contribute to cyber security sustainment and capability development.

Service Features: TBD

Service Flavours: The Service is available as a single flavour.

Available on: Network neutral

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / price: The unit of measure for the Service is Per Service Delivery. Service delivery cost is calculated individually for each service delivery.

SEC019 - Cyber Security Operations Branch SME Service

Service ID: SEC019

Service Name: Cyber Security Operations Branch SME Service

Portfolio Group: Security Services

Service Description: This service combines a number of subservice flavours, each of which provide specialist Operations Branch SME capabilities, principally supporting sustainment activities.

Value Proposition: Support to Cyber Security - Sustainment. Centralised SME services offer good value by combining the synergies of collocated deep skillsets with the efficiency of having cyber specialists available and resourced only when the customer requires them to contribute to cyber security sustainment and capability development.

Service Features: This service provides flexible and bespoke SME solutions and Cyber Security Support comprising:

- Cyber Security Tools Consultancy Service
- Cyber Security Support to Exercises

Service Flavours:

Cyber Security Tools Consultancy Service: Cyber Security Tools Consultancy: Expertise installation, configuration, operation and maintenance in Full Packet Capture, Online Computer Forensics, Online Vulnerability Assessment.

Security logs collection, retention and expertise: A consultancy service able to optimise customer solutions that collect, store, normalize, correlate and review logs from different sources. NCIRC TC has experience in a wide range of tools and data sources, and can tailor a solution for its customers, including provision of expertise in customised development of log parsers, log collection, correlation/SIEM management.

IDS/IPS Management and Tuning: The configuration, maintenance and operations of Intrusion Detection Systems at Network and Host level. These are one of the most important sources of security events for efficient detection. On request, NCIRC TC can provide the expertise to manage and configure customer devices.

Custom Signatures Development: The provision of experts able to write custom signature to detect specific network traffic or system behaviour.

Cyber Security Support to Exercises: Through a single point of contact coordinate the delivery of Cyber Security protection services and provide exercise development support. Activities may include:

- Development of realistic and up to date cross-exercise technical storylines that facilitate the simulation of operational consequence management, simulate impact mission assurance and generate operational-level decision-making
- Support the alignment of cyber elements between exercises
- Support Cyber Security related concept development and experimentation during exercises
- Conduct Type 4 security audits as adversary simulation during exercises
- Provide operational exercise-support services (including CS SL Training Audience)
- Role simulation and exercise control activities

- Coordination of Real life Cyber Security protection services in support of exercises including Gateway Security, Crypto management, Security Certificates, Incident Management and RRT

The scale of these services provided to an exercise activity is subject to appropriate resourcing to meet the requested support, conducted through an agreed program of work.

Available on: Network neutral

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability: Network neutral

Service Restoration: Not applicable.

Service Cost / Price: The unit of measure for the Service is Per Service Delivery. Service delivery cost is calculated individually for each service delivery.

SEC020 - Cyber Security Operations Management Service

Service ID: SEC020

Service Name: Cyber Security Operations Management Service

Portfolio Group: Security Services

Service Description: Cyber Security Internal Services underpin and enable the delivery of the other Cyber Security Service Line (CS SL) Services.

Value proposition: Cyber Security Internal Service facilitate the effective, efficient and resilient delivery of all other CS SL services. The Service provides the essential capabilities that underline the provision of CS SL Cyber Security Services, in particular the people, resource, materiel and management essential to their operational delivery.

Service Features:

Contracted Services Liaison, Management, Change Management, Measurement and Control: Service Operations activities conducted to ensure alignment between NATOs cyber security needs and contractor delivered cyber security Contracted Services delivery, including liaison, management, change management, measurement and control.

CS SL Contingency Planning: Management of the CS SL contribution to NCI Agency Contingency Planning, including Business Continuity Planning and Emergency Recall Planning. Acting as a source of expertise and single point of entry for CS SL Service Level Contingency Planning activities including business impact assessment, risk reduction, mitigation, and liaison with the risk owner.

CS SL Planning, Execution and Management: Planning and execution of CS SL business, procurement, financial, resource, logistics, training coordination, operational deployment planning, travel, and personnel related activities. Review, creation, maintenance, distribution, and advising on CS SL business, financial, resource and personnel planning project plans and documents. Coordination of CS SL logistic requirements, development and management of the CS SL budget, leading the submission of Medium-Term Financial Plan (MTFP) bids and management of all procurement requirements. Includes SL level travel coordination and liaison.

Service Level Management and Reporting: Management of the CS SL contribution to NCI Agency Costed Customer Service Catalogue. Acting as a source of expertise and single point of entry for CS SL Service Level Management activities including catalogue and Service Level Agreement (SLA) reviews, including providing expertise in the formation of metrics and KPIs. Liaison with internal and external customers.

Internal IKM: Cyber Security Information Knowledge Management: Management of the content of all the data-centric CIS Security systems, ensuring the coherence and the accuracy of all the data stores used by CIS Security Capabilities.

Service Request: Inherent to delivery of other Security Services.

Service Flavours: Service is available as a single flavour.

Available on: Network neutral

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC021 - DCIS - Signal Support Group (SSG) Service

Service ID: SEC021

Service Name: Signal Support Group (SSG) Service

Portfolio Group: Security Services

Service Description: The Signal Support Group (SSG) Service supports a deployed JFC Commander by providing general purpose system administration shelters with Environmental Control Unit and a single deployable cyber toolset for monitoring the NU domain against intrusion.

The services listed below are required to assure the continuous operational readiness of the SSG Cyber Defence (CD) Kit:

- Level 3 Engineering Support from Service Lines;
- Microsoft Standard SW Support to ensure sensors are tuned to successfully detect:
  - malicious traffic,
  - email attachments,
  - SQL injection attacks,
  - denial of service attacks, and
  - other cyber threats.
- Maintenance/ annual inspection of:
  - ten (10) General Purpose (GP) Tents and
  - ten (10) Environmental Control Units (ECUs) with required spares;
  - Cost to replace (per year when repair is deemed no longer economically feasible):
  - one (1) sensor kit workstation,
  - one (1) tent, and
  - one (1) ECU.

Value proposition: The service provide SSG with the ability to monitor DCIS services against cyber-intrusion.

Service Features: Customer personnel operate the SSG Cyber-Defence Kit from the Deployed Network Operations Centre (DNOC). The customer will adhere to all Provider processes for cyber services. In the event that the cyber service is impacting the delivery of services to the user community, the provider will inform the customer and the service will be terminated immediately. CS services over and above those described are not currently available for use in DCIS.

CIS Assets:

- DNOC SIEM Server
- Sensor Workstations
- Eclypt Hard Drive (HDD)
- Eclypt External Hard Drive (HDD)
- Eclypt Hard Drive (HDD) Management
- VPN/Firewall

- VPN Concentrator/Firewall
- Network Taps (Datakom)

Non-CIS Assets: General Purpose (GP) Tents. UPS, Racks, Power Strips.

Baseline Changes: Limited to Configuration Changes that do not require hardware replacement of major items. Technical Refresh changes are out of scope of this Service. Changes include:

- Major Changes: completion of Configuration Changes on 50% of all Systems within 1 calendar year. Requirements submission is due 4 months prior to beginning of Financial Year.
- Minor Changes: routine software upgrades, maintenance and security updates, and patches, which will be carried out on a regular basis.

Maintenance: conduct of Preventative Maintenance Inspections (PMI) and routine Corrective Maintenance Inspections (CMI) on all service assets. CMIs undertaken as, and when required, but limited to a maximum value of 5% of the (annual) Service Cost.

Service Flavours: The Service is available as a single flavour.

Available on: NU.

Service Prerequisites:

The cyber service can be deployed and operated by the user after submission of service requests to, and approval of, the NCI Agency.

Standard Service Support Levels:

Service Availability[1] Target: 95% whilst on Ready to Deploy, otherwise 92%.

Service Restoration Period: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is as provided above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is per kit. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

SEC022 - Sensor and Flight Plan Boundary Protection System (BPS) Application Service

Service ID: SEC022

Service Name: Sensor and Flight Plan Boundary Protection System (BPS) Application Service

Portfolio Group: Security Service

Service Description: The Sensor and Flight Plan Boundary Protection System (BPS) is an AirC2 specific service and provides a secure interconnection of Sensor and Flight Plan data sources provided at lower level of classification with the Air Command and Control Service (ACCS). The Service can be utilized for any other Command and Control System used in the Air Domain. The Service is comprised principally of a secured operating platform, data syntax validation and forwarding proxies, and a hardened Application Layer Firewall between those proxies. The Service provides unidirectional data flow from lower to higher level of classification as required to operate ACCS. Extension of this capability with a downgrading filter is planned for a future upgrade.

The BPS falls under the AirC2 governance for programmatic and configuration control aspects. The BPS cyber security function is under oversight of the ACCS Security Accreditation board and a SECAN evaluation is mandatory before an approval to operate can be issued.

Value proposition: Cyber security support to ensure integrity of sensor and flight plan data passed on to the connected Air C2 System while protecting the security boundary of the Air C2 system in regard to the interfaces supported.

Service Features:

The BPS is built on a secured Solaris platform utilizing the NISP Service (APP051) and comprises a message syntax validation through proxies and an Application Layer Firewall as an evaluated security enforcing capability including required secured access to manage required components and interfaces.

The BPS service can be deployed and used in two scenarios:

- Stand-Alone BPS: The BPS supports handling and forwarding Eurocontrol ASTERIX and NATO STANAG 5535 compliant messages, as supported by ASIM (INF028), and it supports ICAO compliant Flight Plan Messages, as required for ACCS (APP050).
- BPS Service combined with ASIM (INF028): extends the BPS to receive, process, and forward all sensor data formats, as supported by ASIM (INF028).

Service Flavours:

BPS specific work packages are available to cover the BPS service installation and the BPS In-Service-Support, which includes level one, two and level three support.

The BPS Service package when combined with ASIM (INF028), the installation and in-service-support packages for both services will be combined.

Available on: The BPS service is available at all NATO classification levels up to NATO Secret at the low side proxy and NATO Secret on the high proxy side.

Service Prerequisites:

APP051 - NISP Service providing the standardized secured operating system

INF028 - ASIM Service when combined with this service

Hardware, software and connection requirements:

- Sensor data available at IP network level
- IP interface as part of the ACCS or Air C2 system
- Three server compatible to run NISP and authorized to host the BPS
- Network infrastructure

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

This page is left blank intentionally

LOGISTIC SERVICES

V3.4

This page is left blank intentionally

LOG001 - CIS Asset & Materiel Management Service

Service ID: LOG001

Service Name: CIS Asset & Materiel Management Service

Portfolio Group: Logistic Services

Service Description: The CIS Asset & Materiel Management Service embraces all of the CIS Asset and Materiel Management activities that the CIS Sustainment Support Centre (CSSC) provides both directly to the Customer and internally as a support function to the Service Lines. CIS Asset and Materiel Management includes CIS equipment codification, database management, inventory management, receipt, dispatch, storage, stock management, warehousing, internal controls, handover takeover, equipment write-on/write-off, support to exercises/operations and disposal coordination. The CSSC performs as the single point of entry for the majority of new CIS equipment procured through common funding of NATO. In addition, CSSC provides Asset Management Subject Matter Expert Services directly to the Customer or internally to the NCI Agency Service Lines.

Value Proposition: The Service provides multiple values:

- Provision of a central hub for most of CIS Asset and Materiel Management activities;
- NATO common funded CIS Equipment is managed and safeguarded throughout the full materiel lifecycle process;
- CIS equipment, and CIS Spares and Consumables for a number of years of Integrated Logistic Support (ILS) of CIS Systems and Capabilities are available to support NATO operations, exercises, and the static infrastructure, with significantly reduced time between requisition and delivery;
- Improvement of the CIS Materiel Management and availability of stock managed items;
- The centralization of the codification, storage, warehousing, receipt, dispatch, transportation, and materiel coordination functions provides cost savings to the NATO Nations. This includes both NSIP as well as the follow on Operations and Maintenance activities;
- In cases where Spares supporting in-service systems are likely to become 'diminished manufacturing availability', they are procured, stored and available for supply by the CSSC Warehouse in order to ensure NATO Business Continuity;
- No longer required equipment can be returned to CSSC, if deemed re-useable, for safe storage ready for return to Service upon requirement reappearance;
- Reduced overall costs per item managed through the stock management process.

Service Features:

- **Codification**: Codification and management of item master data information that is used to support procurement, supply and material management of CIS Equipment purchased using NATO common funding. Codification is used within NATO in order to improve CIS/Non-CIS identification, supply and property accounting. Codification, if carried out correctly, will result in cost savings for NATO as assets will be more efficiently and effectively managed in support of NCI Agency Service provision. The codification is also executed NCI Agency non-CIS equipment and common elements of the AMDC2 System in support of property accounting tasks. Codification is divided into Codification of CIS Assets and Codification of Non-CIS Assets.

- **Planning:** Planning, scheduling, coordination and documentation update for Storage Management and Warehousing Services. Planning, scheduling and coordination for Receipt and Dispatch Services. Planning, scheduling and coordination for asset management SME services.
- **Receipt/Dispatch:** The CSSC performs as the single point of entry for the majority of new CIS equipment procured through common funding of NATO. The Receipt and Dispatch (R/D) activities are an essential element, which supports project execution, service delivery, supply management, asset management and database management activities associated with CIS. CSSC also receives and dispatches non-Common funded materials on request from some Host Nations and MoU organizations. The receiving process, which is managed in the ORACLE Inventory/Order Management database is handled either directly or indirectly by the CSSC Receipt and Dispatch Section within AMSB. This is an Asset Management activity providing identification, serialization and traceability of CIS equipment. CIS Materiel consignments are processed, prepared and dispatched through the R/D section of the AMSB. Dispatch can include freight forwarding, special deliveries, urgent request and courier coordination services. R/D also coordinates the most suitable and cost effective transportation service in conjunction with NSPA. Although NSPA is responsible for the management of transportation of CIS Material on behalf of the NCI Agency, CSSC provides a single point coordination Service to our internal and external customers to ensure that material moves are managed efficiently and effectively. Transportation Requests are received by CSSC RMB, and processed by CSSC AMSB R/D to support the original customer requests (MR/IR/MOI etc.). R/D also manages classified equipment.

- **Storage:** Assets are stored and managed in the CSSC Warehouse as part of the Inventory Project supporting the procurement, supply, exchange, repair and upgrade processes for CIS equipment within the NCI Agency. The Service relates to the CIS requisitioning and supply activities of the NCI Agency.

- **Stock Management:** CSSC provides a Stock Management Service in conjunction with the Inventory Project of the NCI Agency. Planning, scheduling, coordination and documentation update for stock management service. Support to ILS in defining new Stock Management requirement. Supply of CIS stock managed materiel in line with PM requisition requirements. Replenishment activities related to all stock Managed CIS equipment.

- **SME Services**: Provide customers with near real time management of CIS Equipment Account Balances associated with the Custodian Account and Depot Stock Organization Structure. The inventory management service is an essential enabler of material management and property accountability. AMSB in conjunction with RMB provide advice and support to the Operations and Exercise Service Line in the development of CIS Logistics related plans in relation to Exercise and Operational Planning. This planning effort may be dedicated to a specific Exercise/Operation or included within an existing SLA. AMSB provides expert logistics support to projects such as those related to the AMDC2 (AirC2/BMD) in the data capture and inventory setup/management of associated assets. Asset Management and Supply Branch (AMSB) conducts data cleansing activities in support of Projects/Programmes such as EBA and ITM. Although this is not meant to be a day-to-day activity, it is anticipated that this task will continue in excess of 12 months.

- **Inventory Management:** The indirect or direct support is provided to the Custodian Account holder in the completion of the annual inventory activities. The support activities are related

to handling of discrepancies within an account balance list. This can be associated with the annual counting process or for an individual or multiple item loss/damage report.

- **Maintenance Support:** This is a required activity related to the accountability of CIS materiel that is returned by the customer for preventative or corrective maintenance actions. In these cases CSSC will conduct handover/takeover (HO/TO) checks of the property which includes full inventory of materiel prior and after completion of the maintenance activities.
- **Support Planning** The HO/TO is an essential element of inventory checking when equipment is moved from the responsibility of one Sub-PAO to another or back to CSSC. The HO/TO process is required to ensure that common funded equipment is handled in accordance with the Financial Regulations and Asset Management Directives and Procedures.

Service Request: The Service may be requested in multiple ways:

- Identified within SLA / OLA;
- E-mail requests to Resource Management Branch Tasking Cell;
- EBA Project Management Milestone Request;
- EBA Internal Requisition;
- ITSM;
- EBA Work Request;
- EBA Move Order Transfer;
- EBA Internal Requisition;
- E-mail to Resource Management Branch Tasking Cell;
- Materiel Request through iProcurement.

Service Flavours: The Service is available in multiple flavours, depending on the required features and forms of support.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels:

- **In House:** Equipment is stored, maintained and managed at the CSSC main warehouse and released and/or replenished on request from the relevant Service Line/Project Manager.
- **On Site:** Equipment is forward deployed to Buffer Stock locations in order to support the 'urgency' element of spares and consumable supply for Service Lines and PMs.
- **Routine:** Service provided as a routine process associated with standard timelines.
- **Urgent:** Service provided as a prioritized process associated with urgent requirements and timelines.
- **Codification**: All actions required for the execution and management of the codification will be conducted by the codification team within AMSB, CSSC.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG002 - 3rd Level Maintenance of the Communications and Information Systems Service

Service ID: LOG002

Service Name: 3rd Level Maintenance of the Communications and Information Systems Service

Portfolio Group: Logistics Services

Service Description: The 3rd Level Maintenance of the Communications and Information Systems Service entails Preventive (PMI) and Corrective Maintenance (CMI) activities related to the availability of Deployable and other CIS in accordance with the operational requirements of ACO, ACT and Internal Customers. The Service depends upon the type of System and the agreed maintenance schedule required by the customer. The service also entails Equipment TEMPEST Level Testing and 3rd Level Test Equipment Verification and Maintenance.

Value proposition: CIS System Maintenance ensures the availability of capability to the operational users. Preventive Maintenance Schedules ensure that System availability meets provided Customer requirements. Preventive Maintenance and Corrective Maintenance are an important element of any service delivery.

Service Features:

3rd Level Maintenance of CIS:

Features include but are not limited to the following maintenance / engineering activities:

- Maintenance Planning and Coordination;
- Preventive Maintenance Inspection;
- Corrective Maintenance;
- Engineering Modifications to Systems;
- System Testing;
- Materiel Management Associated Maintenance;

The Main Systems covered by this Service include:

Main System	Description
3rd Gen TSGT	Third Generation Transportable Satellite Ground Terminal (TSGT) Services
DSGT	Deployable Satellite Ground Terminal (DSGT) Services
UTSGT	Upgraded Transportable Satellite Ground Terminal (UTSGT) Services
LRLOS	Long Range Deployable Line of Sight (DLOS) Services - LRLOS
SRLOS	Short Range Deployable Line of Sight (DLOS) Services - SRLOS
TLK	Theatre Liaison Kits (TLKs) including BGAN and INMARSAT Handset Services
UHF System	TACSAT (UHF) Services - AN PRC 117-F
HF System	High Frequency (HF) Services
DragonFly	NATO Response Force DCIS - Dragonfly Services
LINC-E	Limited Interim NRF CIS - Expansion (LINC-E) Services
ACP	Afloat Command Platform (ACP) Services
CGS	Communications Gateway Shelters (CGS) Services

NDOG	Mission Anchor Point - NATO Deployed Forces Operational Gateway (NDOG) Services
MDOG	Mission Anchor Point - Mobile Deployed Forces Operational Gateway (MDOG) Services
MPCs/ PRCs	Mission Preparation Centres (MPCs)/ PoP) Replication Centres (PRCs) Support Services
DCEP	Deployable CIS Equipment Pool (DCEP) Services
IMCD	ISAF Mobile CIS Detachment (IMCD)
Mini-PoP	Mini Point of Presence (Mini-PoP)
ILK	ISAF LNO Kits (ILKs)
SSG	Signal Support Group (SSG) Services - SSG/DNOC CYBER DEFENCE (CD) KIT

The various systems comprise different elements of sub-assembly/equipment, which require specific activities to be included as elements of the Service, including:

- Resource Management (Planning and Scheduling) Services (RMS);
- Asset Management Services (AMS);
- Transmission Systems Services (TSS);
- Network & Information System Services (NISS);
- Electronic Maintenance & Testing Services (EMTS);
- CIS Support Equipment Services (CISSES).

The Service is available at central location (CSSC premises at Brunssum) or in deployed locations by CSSC maintenance personnel.

Equipment TEMPEST Level Testing:

In accordance with SDIP-27 standards under the direction of the Cyber Security Service Line (CS SL), CSSC Brunssum maintains one of the two NCIA's TEMPEST facilities conducting tests for CIS items that will be used to process NATO information classified NATO CONFIDENTIAL and above. In more details, the Service provides the following:

- Planning, scheduling, coordination and documentation update for equipment TEMPEST level testing;
- Testing and evaluation of Electric Radiation (ER) signals for CE in order to allocate the appropriate SDIP-27 TEMPEST Level B or C rating;
- Acceptance testing of TEMPEST equipment certified by NATO Approved Suppliers to confirm that the equipment meets the SDIP-27 TEMPEST Level rating allocated;
- Performing mandatory Electrical Safety Inspection for compliance to NEN 3140 (standard for operation of electrical installations - Low voltage).

3rd Level Test Equipment Verification and Maintenance:

Entails initial acceptance testing of new procured Testing Equipment (TE), verification of calibration performed by external institutions, repairs and technical evaluation of items fulfilling NATO standards. It contains the following activities: proofing if the measurements meet all manufacturer specifications (initial and throughout lifecycle), Electrical Safety Inspection for compliance to NEN 3140 (standard for operation of electrical installations - Low voltage), installing manufacturer firmware upgrades, troubleshooting and repairing of defective units. In more details, the Service provides the following:

- Planning, scheduling and coordination for test equipment and verification service;
- Testing instruments to confirm manufacturer specification, performance and functionality;
- Electrical Safety Inspection, which is mandatory for electrical installations and electrical equipment with a nominal operating voltage up to1000 V AC or 1500 V DC;
- Firmware upgrading to ensure TE is updated to the latest version. This fixes bugs and improves performance and security;
- Troubleshooting and Repair of any defects or malfunction;
- Fibre-optic cable repair and testing.

Service Flavours: The Service is available in multiple flavours, depending on combination of required features and location of the Service delivery.

Service Prerequisites:

- Operational Units have completed the Level 1 and 2 Maintenance activities as laid down in the system maintenance guides;
- Operational Units have conducted a full inventory check of the system prior to the Handover Takeover (HO/TO) to the CSSC or Forward Support Point engineering and asset management teams;
- A detailed description of any system fault provided to CSSC with request for deployed maintenance activities;
- Real Life Support provided at deployed locations to enable the conduct of the maintenance.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG003 - 3rd Level Electromagnetic Environmental Effects (E3) and Detection of Radio Frequency Emanations from Electronic Devices Service

Service ID: LOG003

Service Name: 3rd Level Electromagnetic Environmental Effects (E3) and Detection of Radio Frequency Emanations from Electronic Devices Service

Portfolio Group: Logistic Services

Service Description: The Service entails Shielding Effectiveness Testing and maintenance of shielded enclosures to meet the requirements for Electromagnetic Pulse Protection (EMPP), Communication Security (COMSEC), TEMPEST and any other Radio Frequency (RF) interference protection on NATO common static facilities and transportable CIS systems according to MIL-STD-188 125-1/2 and SDIP 29/2. Testing is performed on all NATO shielded enclosures and bunkers, detailed in the ACO Directive 80-052 and all NATO mobile Communications and Information Systems (CIS) embedded in shelters or transportable boxes particularly used with CP0149 at various locations and mission related systems in resolute Support (RS). Detection of Radio Frequency emanations from electronic devices part of the Service entails measurement of extremely low-level RF emanating signals of electrical devices. Within a shielded enclosure, isolated from external RF environmental noise, the RF energy of activated devices can be detected and reported across a wide frequency band. This could be used for individual devices, smaller than 80cm width, up to a system of components.

Value Proposition: Regular inspections / maintenance are required to assure the required Radio Frequency (RF) shielding for all NATO common funded facilities, installations, and CIS (ACE Manual 93-5-1). Inspection serves the purpose to determine whether the facilities, installations and CIS are protected for EMP, COMSEC and TEMPEST. Testing, in accordance with the equivalent standards and the use of associated reference documentation, is the mandated method of managing the risk of damages caused by electromagnetic pulse and of avoiding the capturing and re-transmitting of NATO classified information. Physical and technical inspection of equipment is essential to mitigate the threats associated with the unauthorized implantation of devices, substitution of equipment or manipulation of functionality within electronic equipment to achieve an eavesdropping capability. Without this initial inspection, electronic equipment is not readily possible to determine whether or not the equipment is “fit for purpose” and more importantly whether or not it is “secure”. The level of security being directly correlated to whether or not such equipment contains any embedded malware and / or eavesdropping devices that can be exploited to capture and re-transmit NATO classified information.

Service Features:

E3 service:

- Planning, scheduling and coordination for electromagnetic environmental effects (E3) service.
- Subject Matter Expertise (SME) in RF measurements of attenuation provided by the shield (Shielding Effectiveness [SE] testing) according to the IEEE STD-299, as well on existing and new up-coming projects related to E3 concerns.
- Testing of:
  - Shielded Enclosures;
  - Microwave Sites;

- Satellite Ground Terminal;
- Satellite Ground Segment;
- CIS Systems (TSGT 2nd &TSGT 3rd Generation; SRDLOS; LRDLOS);
- CIS Shelters (HF; Crypto; Helpdesk; AirC2; SIGINT COINS; NNCCRS);

- EMPP testing of Bunkers as detailed in the Allied Command Operation (ACO) Directive 80-52;
- Annual inspection and preventive maintenance according to Allied Command Europe (ACE) Manual 93-5-1.
- Testing of power- and signal-line filters according to MIL-STD-220 and publication method CISPR17.
- Maintenance on manual and pneumatic operated electromagnetic shielded doors.
- Acceptance testing of new and modified installations.
- Technical advice of lightning, surge protection and grounding of CIS networks including power distribution systems.
- Analysis and technical advice related to Electromagnetic Field Safety (EMF) of workplaces imposed by European and derived National Regulations.

Detection of Radio Frequency emanations from electronic devices:

- Planning, scheduling and coordination for detection of RF emanations from ED;
- Active testing technique undertaken by actively stimulating the equipment (i.e. simulating the processing of information);
- Passive testing technique listening to the equipment's electronic operation to detect any unusual or unexplained functionality, emanated signals and/or frequencies;
- Shielded enclosure testing for bugs, excessive Radio Frequencies (RF) emissions at frequencies around GSM 3G/4G and Wi-Fi. Evaluation of Emanating Radiation (ER) for compromising emanation;
- Analysis of the effects of broadcasting audio signals;
- 24h test to look for transmissions of signals without any stimulus.

Service Flavors:

- **In-House Support:** all devices to be tested need to be send to the CSSC and shipped back to the customer;
- **On-Site Support**: testing and measurements performed at the customer's site.

Available on: N/A

Service Prerequisites:

E3 service:

- Installed Operation System (OS) on Servers, Work Stations and Laptops.
- Providing access to OS.

Standard Service support levels: N/A

Service Cost/ Price: Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTHER SERVICES

This page is left blank intentionally

OTH001 - Service Management, Delivery, Measurement, Reporting, and Integration Service

Service ID: OTH001

Service Name: Service Management, Delivery, Measurement, Reporting, and Integration Service

Portfolio Group: Other Services

Service Description: The Service Management, Delivery, Measurement, Reporting, and Integration Service provides a framework to structure IT-related activities and the interactions of IT technical personnel with customers and clients. It focuses on the design, development, and implementation of the ITIL Service Transition and Service Operation processes.

Furthermore, it ensures application of measurement and reporting on process Key Performance Indicators, as well as addressing any process working deficiencies/shortfalls. Service Integration Management (SIM) orchestrates the Service Delivery processes across the NCI Agency and acts as Primary PoC to the customer for Service Delivery matters. The overall aim is to deliver services according to customer expectations, monitoring proactively any relevant deviations and enabling the Operational Management of the NCI Agency SLAs.

Value Proposition: The Service provides a centralised means for effective and efficient management and control of IT processes and procedures, including evaluation and reporting on performance, effectiveness, and efficiency of delivered services, as well as their compliance with the agreed level of quality.

Service Features:

Service Management / Delivery Process Management: provides the service management processes included in ITIL Service Transition and Service Operation: IT Change Management, Service Asset and Configuration Management (SACM), Release and Deployment Management, Request Fulfilment, Event, Incident, Problem and Access Management and their implementation within the ITSM tool.

Measurement and Reporting: relies on measurements and reports from various sources:

- Service Lines, where available and appropriate;
- direct data collection by SMC, where feasible;
- ITSM data interpretation from NS, NR and NNHQ instances;
- data enrichment from mostly legacy CMDBs;
- collection of legacy tools known as Quality of Service Toolset; and
- engineering reporting model promulgated via the Quality Monitoring and Reporting Plan mandated by the CSLA).

Rationalisation and industrialization of the reporting chain will combine the contributions of SMC-TA, ITM, NCI and CP-102 projects, and will therefore continue to be an evolving capability for a relatively long time.

This feature serves multiple purposes:

- fulfil the SLA obligation to report on service performance with prescribed Key Performance Indicators and targets, which comes in the form of monthly reports, quarterly reviews (QSLR – Quality Service Level Reviews) and yearly Quality Monitoring and Reporting Plans;
- to deliver the NCIA internal reporting feed-back to maintain service performance, effectiveness and efficiency in the short, medium and long term;

- to develop, maintain and operate a measurement and reporting chain through service management layers (the system – domain s and enterprise layers) and the various NSIP projects that support them, by combining objective measurements with subjective process traces and customer/user surveys.

Service Integration Management (SIM): performs as the Service Line orchestrator of Service Delivery to the customer and enables the SLAs operational management, which includes Service Delivery cost, processes compliance and performance. It provides the toolset, governance and processes to support seamless, integrated and correlated management of SLA services. It furthermore entails the implementation of Service Improvement Plans coordinated with the SLA service providers, proactive SLA reviews (both internal and external) and the QSLR – Quarterly Service Level Reviews with the customer.

Service Flavours: Service is available in multiple flavours depending on specific arrangements regarding central vs. local contracting, implementation, and execution, as well as on type of reports (automated, fully documented, administrative-driven vs. measurement-driven) and their periodicity (daily, weekly, monthly, yearly).

In the CSLA context, the defined flavours are:

- Formal and fully documented Monthly Report;
- Quarterly Quantitative review; and
- Quarterly Qualitative Review.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Static and Deployable IT infrastructure

Certain limitations apply in NATO Secret and Mission Secret environments, depending on feasibility of measurements and of transfer of data.

Service Prerequisites:

IT Service Management Toolset and its respective CMDB

IT requirements and KPI definitions

Implemented measurement and collection capability

Standard Service Support Levels: In development

Service Availability[1] **Target:** 99.0 %, 99.9 %, and 99.5 **%** for Service Management / Delivery Process Management, Measurement and Reporting, and Service Integration Management respectively.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P1) is 4 hours for Service Management / Process Management and

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Measurement and Reporting features. For Service Integration Management feature the service restoration period for a low incident (i.e. P4) is 3 days, and for a high incident (i.e. P2) is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTH002 - Account Management Service

Service ID: OTH002

Service Name: Account Management Service

Portfolio Group: Other Services

Service Description: Account Management Service provides dedicated Account Managers to each NCI Agency eligible customer. Account Manager is responsible for Customer engagement, and establishes and maintains the Agency relationships with a customer or group of customers. They serve as the principal interface between the customer and the delivery of Agency services, through understanding the customer's demands and ensuring these are translated into clear requirements for capability or service In addition they , plan how to meet these demands, and generate requirements for the Agency.

Value proposition: The Service provides a principal focus and entry point into the Agency for routine business. By assisting the Customer in developing and refining the requirements before acting on these requests, and monitoring their progress through the Agency Business Processes, Account Management Service enables an optimal delivery of requested capability and services.

Service Features:

Establishment and maintenance of a customer-account manager relationship.

Identification of new business opportunities within existing accounts.

Managing Customer Requests: the Account Manager will receive customer requests, preferably via an Agency Customer Request Form and subsequently manage the prioritisation of this request through the Agency Business Intake process, communicating with the customer as appropriate to keep them fully informed.

Coordination of Price Proposals, Service Level Agreements, and Service Support Packages: the Account manager is the customer and Agency focal point for tracking the production, issue and acceptance of formal offers from the Agency for capability delivery or service delivery.

Problem Management: the Account Manager understands the Customer Requirement and any agreement in place to meet that requirement and coordinates Agency responses to the Customer during problem management.

Reporting: the Account Manager coordinates project and SLA reporting as required.

Service Request: The Service is provided as business as usual through a formal and informal request process from the customer that results in activity and action delivered by the Account Manager, which is charged through the appropriate billing vehicle**.**

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTH003 - AirC2 In Service Support Program of Work (ISS POW) General Support Service

Service ID: OTH003

Service Name: AirC2 In Service Support Program of Work (ISS POW) General Support Service

Portfolio Group: Other Services

Service Description: The Service entails services provided to ACO as a part of the AirC2 ISS POW that are not directly related to individual application services, due to the generic nature of performed activities to support services across a number of systems.

Value proposition: The service enables the overall delivery of the in-service-support for all AirC2 applications and systems.

Service Features: The service entails the following activities:

- Contract and licence management;
- Interoperability management;
- Security management;
- Support to governance meetings and NATO committees and Working Groups;
- Support to Platforms and Tools;
- Development of POW related price proposals.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTH004 - DCIS - Management Support Service

Service ID: OTH004

Service Name: Deployable CIS Management Support Service

Portfolio Group: Other Services

Service Description: The NSII Ops Programme Service Management (OPSM) Office manages all aspects for the delivery of services as described in the Service Level Agreement.

Value proposition: The service provides management of all services, providing confidence to the customer that services delivery will continue as described in the respective Service Level Agreement (SLA).

Service Features: The Service has the following features:

- Availability Management;
- Incident Management;
- Problem Management;
- Delivery Management;
- Change Management;
- Obsolescence Management;
- Information Management;
- Transition Management for projects that are in support of the customer, but funded through the NATO Security and Investment Program (NSIP).

Service Flavours:

Deployable CIS Service

In-garrison CIS Service

Available on: N/A

Service prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.